华章数学译丛

36

A First Course in Abstract Algebra with Applications

(Third Edition)

抽象代数基础教程

（原书第3版）

（美）Joseph J. Rotman 著
伊利诺伊大学

李样明 冯明军 译

PRENTICE HALL

机械工业出版社
China Machine Press

VISIT…

LANZAROTE Caliente.COM

目　　录

译者序

译者简介

前言

教学大纲建议

致读者

特殊符号

第 1 章　数论 …… 1

1.1　数学归纳法 …… 1

1.2　二项式定理与复数 …… 13

1.3　最大公因子 …… 26

1.4　算术基本定理 …… 40

1.5　同余 …… 42

1.6　日期与天数 …… 55

第 2 章　群Ⅰ …… 61

2.1　一些集合理论 …… 61

2.1.1　函数 …… 63

2.1.2　等价关系 …… 71

2.2　置换 …… 76

2.3　群 …… 89

2.4　子群和拉格朗日定理 …… 104

2.5　同态 …… 112

2.6　商群 …… 121

2.7　群作用 …… 136

2.8　用群计算 …… 148

第 3 章　交换环Ⅰ …… 154

3.1　基本性质 …… 154

3.2　域 …… 163

3.3　多项式 …… 166

3.4　同态 …… 172

3.5　从数到多项式 …… 179

3.6　唯一分解 …… 196

3.7　不可约性 …… 200

3.8　商环与有限域 …… 207

3.9　一个数学历程 …… 218

3.9.1　拉丁方 …… 218

3.9.2　幻方 …… 221

3.9.3　试验设计 …… 224

3.9.4　射影平面 …… 226

第 4 章　线性代数 …… 229

4.1　向量空间 …… 229

4.2　欧氏作图 …… 254

4.3　线性变换 …… 262

4.4　特征值 …… 275

4.5　码 …… 287

4.5.1　分组码 …… 287

4.5.2　线性码 …… 292

4.5.3　译码 …… 305

第 5 章　域 …… 312

5.1　经典公式 …… 312

5.2　一般五次方程的不可解性 …… 325

5.2.1　求根公式与根式可解性 …… 332

5.2.2　二次多项式 …… 333

5.2.3　三次多项式 …… 333

5.2.4　四次多项式 …… 333

5.2.5　用群论语言的叙述 …… 334

5.3　结束语 …… 341

第 6 章　群Ⅱ …… 344

6.1　有限阿贝尔群 …… 344

6.2　西罗定理 …… 354

6.3　装饰的对称 …… 363

第 7 章　交换环Ⅱ …… 378

7.1　素理想和极大理想 …… 378

7.2　唯一分解 …… 382

7.3 诺特环 …… 390
7.4 簇 …… 394
7.5 广义的除法算式 …… 407
7.5.1 单项式序 …… 408
7.5.2 除法算式 …… 412
7.6 格罗布纳基 …… 416
附录 A 不等式 …… 425
附录 B 伪码 …… 427
部分习题提示 …… 429
参考文献 …… 439
索引 …… 442

第1章 数　　论

→1.1 数学归纳法

证明的方法有许多种，数学归纳法就是其中之一．我们先来谈谈数学归纳法不能用在什么方面．在自然科学中，归纳推理是用来断言频繁观察到的现象将一直发生的．因此，人们之所以说太阳明天早上会升起，是因为每天早上太阳都升起了．但在数学中这不是合理的证明，因为即使一种现象发生了多次，也不意味着它会永远发生．然而，归纳推理在数学中就像在自然科学中一样仍然是重要的，因为观察数据中的样本可以帮助我们猜想什么事情具有普遍性．

另一方面，一个合理的猜测也可能是不正确的．例如，n 个平面最多可以把$\mathbb{R}^3$(3-维空间)分割成几个区域？两个不平行的平面可以把$\mathbb{R}^3$分割成4个区域，三个平面可以把$\mathbb{R}^3$分割成8个区域(卦限)．对于更小的 n，我们注意到一个平面把$\mathbb{R}^3$分割成2个区域，而若 $n=0$，则$\mathbb{R}^3$根本没有被分割：只有一个区域．因此，对于 $n=0$，1，2，3，区域的最大个数分别是1，2，4，8．我们自然会猜测可以选取 n 个平面把$\mathbb{R}^3$分割成 2^n 个区域．但是，实际上任意四个平面最多可以把$\mathbb{R}^3$分割成15个区域！

在进一步叙述之前，我们先给出一些标准术语的含义．数0，1，−1，2，−2，3，…称为**整数**．所有整数构成的集合记为$\mathbb{Z}$(来自德语中的Zahl，意思是数)：

$$\mathbb{Z}=\{0,1,-1,2,-2,3,\cdots\}.$$

自然数集是由所有满足 $n\geqslant 0$ 的整数 n 构成的：

$$\mathbb{N}=\{n\in\mathbb{Z}: n\geqslant 0\}=\{0,1,2,3,\cdots\}.$$ 1

→ **定义** *设 n，d 是两个整数，如果存在整数 a，使得 $n=da$，则称 d 是 n 的一个***因子**．*自然数 n 称为***素数**[⊖]，*如果 $n\geqslant 2$ 且它的因子只有 ± 1 和 $\pm n$；如果自然数 $n\geqslant 2$ 不是素数，则称它为***合数**．

若正整数 n 是合数，则有分解 $n=ab$，其中 $a<n$ 和 $b<n$ 是正整数，这里用不等号表示除去无意义的分解 $n=n\times 1$．前面的一些素数是2，3，5，7，11，13，17，19，23，29，31，37，41，…．推论1.33将证明此数列是永不终止的．

考虑如下论断：对每个正整数 n，

$$f(n)=n^2-n+41$$

都是素数．对 $n=1$，2，3，…，40，$f(n)$取值如下：

41，43，47，53，61，71，83，97，113，131，
151，173，197，223，251，281，313，347，383，421，
461，503，547，593，641，691，743，797，853，911，
971，1033，1097，1163，1231，1301，1373，1447，1523，1601．

虽然证明这些数都是素数是一项冗长乏味的工作，但并不很难(见命题1.3)．由归纳推理我们猜测所有形如 $f(n)$的数都是素数．然而，下一个数 $f(41)=1681$ 不是素数，因为 $f(41)=$

⊖ 如果素数包含1，则许多有关素数的定理将会变得更加复杂，所以规定1不是素数．

$41^2-41+41=41^2$ 显然是合数．因此，归纳推理不适用于数学证明．

下面再给出一个更好的例子(最先见于 W. Sierpinski 的一篇文章)．我们回忆一下，**完全平方数**是指形如 n^2 的数，其中 n 是整数．前面的一些完全平方数是 0，1，4，9，16，25，36，…．对每个 $n\geqslant 1$，考虑命题

$$S(n):991n^2+1 \text{ 不是完全平方数.}$$

这个关于 n 的命题 $S(n)$ 对很多 n 都是成立的．实际上，使 $S(n)$ 不成立的最小数是

$$n=12\,055\,735\,790\,331\,359\,447\,442\,538\,767$$
$$\approx 1.2\times 10^{28}.$$

方程 $m^2=991n^2+1$ 是 **佩尔(Pell)方程** ($m^2=pn^2+1$，其中 p 是素数)的一个特例，且存在求它的
2 所有可能解的方法．佩尔方程的另一个更好的例子与素数 $p=1\,000\,099$ 相关，使 $1\,000\,099n^2+1$ 为完全平方数的最小的 n 有 1116 位数字．地球年龄的粗略估计是 100 亿年，或 3.65×10^{12} 天，这个数相对于 1.2×10^{28} 来说是微不足道的，更不用说相对于 10^{1115} 了．如果有人从地球产生的第一天开始，在第 n 天验证命题 $S(n)$ 是否成立，那么此命题成立的证据与太阳明天早上一定会升起这一命题的证据一样多．然而 $S(n)$ 中还是有些命题不成立！

作为最后一个例子，我们考虑下述命题，即众所周知的**哥德巴赫猜想**：任何一个大于或等于 4 的偶数 m 都是两个素数的和．还没有人能举出哥德巴赫猜想的反例，但也没有人证明它成立．目前，哥德巴赫猜想被证实对所有满足 $m<10^{13}$ 的偶数 m 都成立，并且陈景润证明了每个充分大的偶数 m 都可以写成 $p+q$ 形式，其中 p 是素数，q“几乎”是素数，也就是说，q 是一个素数或者是两个素数的乘积．然而，即使有这么多正面的证据，数学家们也没有因此就说哥德巴赫猜想对一切偶数 m 都成立．

我们已经明白了(数学)归纳法不能用在什么方面，现在就来讨论归纳法能用在什么方面．数学归纳法所依据的原理是自然数集的下述性质(通常称为良序原则)．

最小整数公理 *自然数集* $\mathbb{N}$ *的每个非空*[⊖] *子集* C *中都含有一个最小整数．*

尽管最小整数公理不能被证明(它是在分析整数是什么时产生的)，但它的确是有道理的．考虑下述过程：检查 0 是否属于 C；若是，则 0 是 C 中的最小整数．否则，检查 1 是否属于 C；若是，则 1 是 C 中的最小整数；若不属于，则检查 2．如此继续下去，直到有一个数属于 C．因为 C 是非空的，所以最终能找到一个最小整数．

命题 1.1(最小反例) *设* k *是一个自然数，*$S(k)$，$S(k+1)$，…，$S(n)$，…*是一组命题．若这些命题中有一些是假命题，则一定能找到第一个假命题．*

证明 设 C 是由使 $S(n)$ 为假命题的所有自然数 $n\geqslant k$ 构成的集合．根据假设可知，C 是 $\mathbb{N}$ 的非空子集．由最小整数公理可知，C 中有一个最小整数 m，即 $S(m)$ 是第一个假命题． ■

这个看似无关紧要的命题其实是很有用的．

3 → **定理 1.2** *每个整数* $n\geqslant 2$ *或是素数或是一些素数的乘积．*

证明 假设结论不成立，则存在“反例”，即一定存在整数 $n\geqslant 2$ 既不是素数也不是一些素数的乘积．根据最小反例，可令 m 是这些整数中最小的一个．因为 m 不是素数，则 m 是合

⊖ 称集合 C 是非空的，是指 C 中至少有一个整数．

数，因此存在因子分解 $m=ab$，$2\leqslant a<m$，$2\leqslant b<m$（因为 a 是整数，所以由 $1<a$ 可知 $2\leqslant a$）．因为 m 是最小反例，所以 a 和 b 都使定理成立，即

$$a=pp'p''\cdots,\quad b=qq'q''\cdots,$$

其中因子 p，p'，p''，…和 q，q'，q''，…都是素数．因此

$$m=ab=pp'p''\cdots qq'q''\cdots$$

是一些（至少两个）素数的乘积，矛盾．⊖ ■

命题 1.3　*设 $m\geqslant 2$ 是正整数，若 m 不能被任何满足 $p\leqslant\sqrt{m}$ 的素数 p 整除，则 m 是一个素数．*

证明　若 m 不是一个素数，则 $m=ab$，其中 a，b 是正整数，$a<m$，$b<m$．若 $a>\sqrt{m}$，$b>\sqrt{m}$，则 $m=ab>\sqrt{m}\sqrt{m}=m$，矛盾．因此，不妨假设 $a\leqslant\sqrt{m}$．根据定理 1.2 可知，a 或者是一个素数，或者是一些素数的乘积，且 a 的任何素因子 p 也是 m 的一个素因子．这样，如果 m 不是素数，则它有一个"小"素因子 p，即 $p\leqslant\sqrt{m}$．由逆否命题法知，如果 m 没有小素因子，则 m 是素数． ■

命题 1.3 可以用来证明 991 是一个素数．这只需检验 991 是否能被某个素数 p 整除，且 $p\leqslant\sqrt{991}\approx 31.48$．若 991 不能被 2，3，5，…，31 整除，则它是素数．这样的素数有 11 个，经检验（用长除法）它们都不是 991 的因子．我们还可以用同样的方法检验 1 000 099 是一个素数，但验算过程更长，因为它的平方根比 1000 还要大．另外，要证明所有 $f(n)=n^2-n+41$（$1\leqslant n\leqslant 40$）都是素数也是一件冗长乏味但并不困难的事情．

数学归纳法是最小反例的一种形式，但它使用起来更加方便．数学归纳法的基本思想无非如此：想象一架通往天空的梯子，如果它的第一个阶梯是白色的，且白色阶梯上方的那个阶梯也是白色的，则这架梯子的所有阶梯都是白色的（据 Francesco Maurolico 在 1557 年的记 4
载，这一思想可以追溯到 1321 年的 Levi ben Gershon，他对归纳法作了清楚的阐述，且被帕斯卡引用过）．例如，命题"对所有的 $n\geqslant 1$，$2^n>n$"可以视为一组无穷命题（通向天空的一架梯子）：

$$2^1>1;2^2>2;2^3>3;2^4>4;2^5>5;\cdots.$$

显然，$2^1=2>1$．如果 $2^{100}>100$，则

$$2^{101}=2\times 2^{100}>2\times 100=100+100>101.$$

对于指数 100 没有什么好奇怪的，一旦我们到达了任何一个阶梯，就可爬上它上面的那个阶梯．这一论述将在命题 1.5 中正式给出．

→　**定理 1.4（数学归纳法）**⊜　*给定一组关于自然数 $n\geqslant 1$ 的命题 $S(n)$，假设*

（i）**基础步骤**：*$S(1)$ 成立；*

⊖ 命题"P 推出 Q"的逆否命题是命题"（非 Q）推出（非 P）"．例如，"若级数 $\sum a_n$ 收敛，则 $\lim\limits_{n\to\infty}a_n=0$"的逆否命题是"若 $\lim\limits_{n\to\infty}a_n\neq 0$，则 $\sum a_n$ 发散"．若一个命题是成立的，则它的逆否命题也是成立的；反之，若逆否命题是成立的，则原命题也是成立的．这种证明策略是证明原命题的逆否命题．尽管一个命题与它的逆否命题在逻辑上是等价的，但有时证明逆否命题会更方便一些．此方法称为间接证明法或反证法．

⊜ "归纳"（induction）这一单词的拉丁词根的意思是"导致"，即"流行去做什么"或"影响"．这个词意是恰当的，因为第 n 个命题影响第 $n+1$ 个命题．

(ii)**归纳步骤**：若 $S(n)$ 成立，则 $S(n+1)$ 也成立.

那么对一切整数 $n \geqslant 1$，$S(n)$ 都成立.

证明 我们必须证明由使 $S(n)$ 为假命题的所有正整数 n 构成的集合 C 是空集.

相反地，假设 C 非空，则存在第一个假命题 $S(m)$. 因为 $S(1)$ 成立，所以由(i)必有 $m \geqslant 2$，这说明 $m-1 \geqslant 1$，因此命题 $S(m-1)$ 存在[没有命题 $S(0)$]. 因为 m 是最小反例，所以 $m-1$ 必使定理成立，即 $S(m-1)$ 成立. 但由(ii)知，$S(m)=S([m-1]+1)$ 成立，这是一个矛盾. 这样我们证明了 C 是空集，因而所有命题 $S(n)$ 成立. ■

现在我们来看看如何应用数学归纳法.

命题 1.5 对所有整数 $n \geqslant 1$ 都有 $2^n > n$ 成立.

证明 第 n 个命题 $S(n)$ 是

$$S(n): 2^n > n.$$

对应于定理 1.4 中的两个假设，用归纳法证明需要两个步骤.

基础步骤. 因为 $2^1=2>1$，所以第一个命题

$$S(1): 2^1 > 1$$

5 成立.

归纳步骤. 若 $S(n)$ 成立，则 $S(n+1)$ 也成立；即利用**归纳假设** $S(n)$，我们必须证明

$$S(n+1): 2^{n+1} > n+1.$$

若 $2^n > n$ 成立，则在不等式两边同时乘以 2，根据附录 A 中的命题 A.2，下述不等式成立：

$$2^{n+1} = 2 \times 2^n > 2n.$$

因为 $2n=n+n \geqslant n+1$（因为 $n \geqslant 1$），故 $2^{n+1} > 2n \geqslant n+1$，这正是我们要证明的.

证明了基础步骤和归纳步骤之后，我们可以得出结论：对所有 $n \geqslant 1$，$2^n > n$ 都成立. ■

最小整数公理是合理的，同样，归纳法也是合理的. 假设一组给定的命题 $S(1)$，$S(2)$，$S(3)$，…具有以下性质：只要 $S(n)$ 成立就有 $S(n+1)$ 成立. 这时，如果 $S(1)$ 成立，则 $S(2)$ 成立；$S(2)$ 成立推出 $S(3)$ 成立；$S(3)$ 成立推出 $S(4)$ 成立，等等. 归纳法用归纳步骤代替了“等等”，这保证了对每个 n，由命题 $S(n)$ 可以顺利地过渡到下一个命题 $S(n+1)$.

在我们更详细地阐述归纳法之前，先来看两点说明. 第一，我们必须同时证明基础步骤和归纳步骤，仅证明其中一个是不够的. 例如，考虑命题 $S(n)$: $n^2=n$. 基础步骤成立，但我们不能证明其归纳步骤也成立(当然，对一切 $n>1$，命题均不成立). 再看另一个命题 $S(n)$: $n=n+1$，容易看出其归纳步骤成立：若 $n=n+1$，则由命题 A.2 知，两边加上 1 得 $n+1=(n+1)+1=n+2$，即下一个命题 $S(n+1)$ 成立. 但是基础步骤不成立(当然所有命题都不成立).

第二，许多人初次看归纳法时，会怀疑归纳步骤是循环推理：我们利用 $S(n)$，而这却是我们想要证明的！仔细分析可知，这根本不会发生. 归纳步骤本身并没有证明 $S(n+1)$ 成立，而是说：若 $S(n)$ 成立，则 $S(n+1)$ 也成立. 换句话说，归纳步骤证明了“若 $S(n)$ 成立，则 $S(n+1)$ 成立”这一结论的正确性. 这个结论正确与命题结论正确不是同一回事. 例如，考虑两个命题：“每次考试你的成绩都是满分”和“这门功课你的成绩是 A”. “若你的所有考试都考得最好，则你会获得这门功课的最高分”这一结论是成立的. 但是，这不是说你这门课的成绩

必定得 A. 对上述讨论我们还给出一个数学例子："若 $n=n+1$，则 $n+1=n+2$"这一结论是对的，但"$n+1=n+2$"却是错的. 6

命题 1.6 对每个整数 $n\geqslant 1$，有 $1+2+\cdots+n=\frac{1}{2}n(n+1)$.

证明 对 $n\geqslant 1$ 用归纳法证明.

基础步骤. 若 $n=1$，则左边等于 1，右边等于$\frac{1}{2}\times 1\times(1+1)=1$，命题成立.

归纳步骤. 为便于看出我们要证明什么，把第$(n+1)$个命题写作 $S(n+1)$. 我们必须证明

$$S(n+1):1+2+\cdots+n+(n+1)=\frac{1}{2}(n+1)(n+2).$$

根据归纳假设，即利用 $S(n)$，左边是

$$[1+2+\cdots+n]+(n+1)=\frac{1}{2}n(n+1)+(n+1),$$

而由高中代数知$\frac{1}{2}n(n+1)+(n+1)=\frac{1}{2}(n+1)(n+2)$. 由归纳法知，公式对一切 $n\geqslant 1$ 都成立. ■

这里有一个关于高斯小时候的故事(也许这个故事根本就没发生过)：他的一位老师要求学生们从 1 加到 100，希望借此腾出时间做其他事情，但是高斯很快就说出答案是 5050. 他把从 1 到 100 的所有整数的和记为 s，即 $s=1+2+\cdots+99+100$. 当然，$s=100+99+\cdots+2+1$. 把这两个等式巧妙地排列如下：

$$s=1+2+\cdots+99+100$$
$$s=100+99+\cdots+2+1$$

相加得

$$2s=101+101+\cdots+101+101,$$

和 101 出现了 100 次. 解得 $s=\frac{1}{2}\times(100\times 101)=5050$. 用任意数 n 代替 100，这个方法也行得通(没有用到归纳法). 这个方法不仅为命题 1.6 提供了一个新的证明，而且还展示了这个公式是怎样被发现的.[⊖]

在归纳证明中，基础步骤并不总是很简单的. 事实上，所有下列可能的情况都会发生：或者两个步骤都很容易，或者两个步骤都很难，或者其中一个比另一个难. 7

命题 1.7 若假设有导数的乘法法则$(fg)'=f'g+fg'$，则对一切整数 $n\geqslant 1$ 有

$$(x^n)'=nx^{n-1}.$$

证明 对 $n\geqslant 1$ 用归纳法证明.

基础步骤. 若 $n=1$，则我们要问是否有$(x)'=x^0\equiv 1$. 由导数的定义知

$$f'(x)=\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}.$$

⊖ 实际上，这个公式可以追溯到至少一千年以前(见习题 1.11). 对任一固定整数 $k\geqslant 1$，Alhazen(Ibn al-Haytham)(965—1039)发现了求

$$1^k+2^k+\cdots+n^k$$

的一种几何方法(见习题 1.12).

当 $f(x)=x$ 时，有

$$(x)'=\lim_{h\to 0}\frac{x+h-x}{h}=\lim_{h\to 0}\frac{h}{h}=1.$$

归纳步骤．我们必须证明$(x^{n+1})'=(n+1)x^n$．因为基础步骤已经被证明，所以可以利用归纳假设$(x^n)'=nx^{n-1}$以及$(x)'=1$．由于$x^{n+1}=x^n x$，则由导数的乘法法则可知

$$\begin{aligned}(x^{n+1})'&=(x^n x)'=(x^n)'x+x^n(x)'\\&=(nx^{n-1})x+x^n 1=(n+1)x^n.\end{aligned}$$

于是得出结论：对所有$n\geqslant 1$，有$(x^n)'=nx^{n-1}$成立． ■

→ **注** 最小整数公理不仅适用于N，而且还适用于N的任意非空子集Q(事实上，命题1.1的证明就利用了这个公理对$Q=\{n\in\mathbb{N}: n\geqslant 2\}$也成立的事实)．用归纳法的语言，这就是说，基础步骤可以从任意一个正整数k开始，而不一定要从$k=1$开始．然后结论是命题$S(n)$对所有$n\geqslant k$都成立．最小整数公理也适用于更大的集合$Q_k=\{n\in\mathbb{Z}: n\geqslant k\}$，其中$k$是任意整数，可能为负整数．若$C$是$Q_k$的非空子集，且$C\cap\{k, k+1, \cdots, -1, 0\}$[⊖]是非空的，则这个有限集合含有一个最小整数，它是C中的最小整数．若$C\cap\{k, k+1, \cdots, -1, 0\}$是空集，则$C$实际上是N的一个非空子集，且由原来的公理得到$C$中的最小数．用归纳法的语言，这就是说，基础步骤可以从0开始，或者从任意整数k开始，k可能是负数[当然，假设存在第k个命题$S(k)$]．例如，若我们有命题$S(-1)$，$S(0)$，$S(1)$，…，则基础步骤可以从$n=-1$开始，此时

8 的结论是命题$S(n)$对所有$n\geqslant -1$都成立．

下面是基础步骤从$n=5$开始的一个例子．考虑命题

$$S(n): 2^n>n^2.$$

当n很小时，命题不成立：若$n=2$或4，则$2^n=n^2$；若$n=3$，则左边是8，比右边9更小．但是，$S(5)$成立，因为$32>25$．

命题 1.8 对所有整数$n\geqslant 5$，有$2^n>n^2$．

证明 我们刚才已经验证了$S(5)$成立．在证明

$$S(n+1): 2^{n+1}>(n+1)^2$$

的过程中，可假设$n\geqslant 5$ (实际上，只需$n\geqslant 3$)并进行归纳假设．在$2^n>n^2$两边同时乘以2可得

$$2^{n+1}=2\times 2^n>2n^2=n^2+n^2=n^2+nn.$$

因为$n\geqslant 5$，所以$n\geqslant 3$，这样

$$nn\geqslant 3n=2n+n\geqslant 2n+1.$$

因此

$$2^{n+1}>n^2+nn\geqslant n^2+2n+1=(n+1)^2.$$ ■

至此，我们已经利用归纳法证明了一些次要的结果，现在用归纳法证明一些更具实质性的结论．首先观察到，若x，y都是正实数，则由恒等式

$$(x+y)^2=(x-y)^2+4xy$$

⊖ 若C，D都是集合X的子集，则它们的交是由X中所有既属于C又属于D的x构成的集合，记为$C\cap D$.

得

$$\left[\frac{1}{2}(x+y)\right]^2 = xy + \left[\frac{1}{2}(x-y)\right]^2.$$

于是

$$\frac{1}{2}(x+y) \geqslant \sqrt{xy}, \tag{1}$$

其中$\left[\frac{1}{2}(x-y)\right]^2$表明了为什么一般情况下是不等式而不是等式. 若等式成立，则$\left[\frac{1}{2}(x-y)\right]^2=0$，$x=y$. 反之，若$x=y$，则得等式$\left[\frac{1}{2}(x+x)\right]^2=xx=x^2$，因为$\left[\frac{1}{2}(x-x)\right]^2=0$. 下面是这一观察结果的一个应用.

回忆**双曲余弦**的定义为$\cosh(x)=\frac{1}{2}(e^x+e^{-x})$. 因为$e^xe^{-x}=1$，所以由不等式(1)知对所有$x$有

$$\cosh(x) \geqslant 1,$$

等式成立当且仅当$e^x=e^{-x}$，即$\cosh(x)=1$当且仅当$e^{2x}=1$，所以$\cosh(x)=1$当且仅当$x=0$. 9

定义　给定正数$a_1, a_2, \cdots, a_n$，它们的**算术平均数**是指$(a_1+a_2+\cdots+a_n)/n$，它们的**几何平均数**是指$\sqrt[n]{a_1a_2\cdots a_n}$.

我们刚才已经证明了两个正数a_1, a_2的算术平均数比几何平均数大，只有当$a_1=a_2$时它们的算术平均数与几何平均数才相等. 以下要把这个结果推广到多个正数上，先看一个基本引理.

引理 1.9　若$0<m<1<M$，则$m+M>1+mM$.

证明　因为正数的积为正数，所以

$$(1-m)(M-1) = M-1-mM+m$$

是正数. 因此$M+m>1+mM$，证毕. ■

例如，若θ是一个锐角，即$0°<\theta<90°$，则$0<\cos\theta<1$，所以$1<1/\cos\theta=\sec\theta$. 因此有不等式$0<\sin\theta<1<\sec\theta$，所以由引理1.9得不等式(其中$\theta$是锐角)

$$\sin\theta + \sec\theta > 1 + \sin\theta\sec\theta = 1 + \tan\theta.$$

引理 1.10　若$k_1, \cdots, k_n$都是正数且$k_1\cdots k_n=1$，则$k_1+\cdots+k_n\geqslant n$. 另外，等式成立当且仅当$1=k_1=\cdots=k_n$.

证明　显然，若所有$k_i=1$，则$k_1+\cdots+k_n=n$. 因此，为证明这两个命题，只需证明若$k_1\cdots k_n=1$，且不是所有的$k_i=1$，则$k_1+\cdots+k_n>n$. 我们对$n\geqslant 2$用归纳法证明之.

基础步骤. 现在$k_1k_2=1$. 若k_1, k_2都大于1，则$k_1k_2>1$. 若k_1, k_2都小于1，则$k_1k_2<1$. 因此，可假设$0<k_1<1<k_2$，由引理1.9得$k_1+k_2>1+k_1k_2=2$.

归纳步骤. 假设$k_1\cdots k_{n+1}=1$，其中$k_1, \cdots, k_{n+1}$都是正数. 若所有$k_i\geqslant 1$，则由不是所有$k_i=1$得$k_1\cdots k_{n+1}>1$，矛盾. 因此，可进一步假设某个$k_i<1$. 为了记号上的方便，设$k_1<1$. 类似地，可以假设$k_{n+1}>1$. 定义

$$a = k_1k_{n+1}.$$

根据引理 1.9，$k_1+k_{n+1}>1+k_1k_{n+1}=1+a$，所以两边都加上 $k_2+\cdots+k_n$ 得

$$k_1+k_2+\cdots+k_n+k_{n+1}>1+a+k_2+\cdots+k_n. \tag{2}$$

只剩下证明 $1+a+k_2+\cdots+k_n\geqslant n+1$ 了[因为(2)是严格不等式]. 注意 $ak_2\cdots k_n=k_1k_2\cdots k_{n+1}=1$. 若 $a=1=k_2=\cdots=k_n$，则 $1+a+k_2+\cdots+k_n=n+1$，证毕. 否则，应用归纳假设得

10 $a+k_2+\cdots+k_n>n$，因而 $1+a+k_2+\cdots+k_n>n+1$. ■

定理 1.11（平均不等式） 若 a_1，a_2，…，a_n 都是正数，则

$$(a_1+a_2+\cdots+a_n)/n\geqslant\sqrt[n]{a_1a_2\cdots a_n};$$

另外，等式成立当且仅当 $a_1=a_2=\cdots=a_n$.

证明 定义 $G=\sqrt[n]{a_1a_2\cdots a_n}$，并对所有 i 定义 $k_i=a_i/G$. 于是 $k_1k_2\cdots k_n=a_1a_2\cdots a_n/G^n=1$，所以根据引理 1.10 有 $k_1+k_2+\cdots+k_n\geqslant n$，即 $a_1+a_2+\cdots+a_n\geqslant nG$，或

$$(a_1+a_2+\cdots+a_n)/n\geqslant G=\sqrt[n]{a_1a_2\cdots a_n}.$$

另外，引理 1.10 指出等式成立当且仅当所有 $k_i=1$，即等式成立当且仅当所有 a_i 相等(等于 G). ■

这个不等式在习题 1.26 中用来证明一个等周不等式：在周长相等的所有三角形中，等边三角形的面积最大.

还有另一种归纳法，通常称为**第二归纳法**，用起来也很方便.

定义 自然数 $n\geqslant1$ 的**前导**是指：满足 $k<n$ 的自然数 k，即 0，1，2，…，$n-1$(0 没有前导).

→ **定理 1.12（第二归纳法）** 设 $S(n)$是关于正整数 n 的一组命题，并设

(i)$S(1)$成立，且

(ii)若对 n 的所有前导 k 有 $S(k)$成立，则 $S(n)$也成立.

则 $S(n)$对一切整数 $n\geqslant1$ 都成立.

证明 只需证明不存在使 $S(n)$为假命题的正整数 n，即证明由使 $S(n)$为假命题的所有正整数 n 构成的集合 C 是空集.

相反地，假设 C 非空，则存在最小反例 m，即存在第一个假命题 $S(m)$. 因为由(i)知$S(1)$成立，所以 $m\geqslant2$. 又因为 m 是最小反例，所以对所有满足 $k<m$ 的 k 定理成立，即对 m 的一切前导 k 有 $S(k)$成立，此时由(ii)知 $S(m)$成立，矛盾. 于是我们证明了 C 是空集，从而所有命题 $S(n)$成立. ■

利用第二归纳法可以给出定理 1.2 的另一个证明. 与用第一归纳法类似，基础步骤不必从

11 1 开始.

→ **定理 1.13（=定理 1.2）** 每一个整数 $n\geqslant2$，或者是素数，或者是素数的乘积.

证明[⊖] 基础步骤. 当 $n=2$ 时，因为 2 是素数，所以命题成立.

归纳步骤. 当 $n\geqslant2$ 是素数时命题成立；当 $n\geqslant2$ 不是素数时，$n=ab$，其中 $2\leqslant a<n$，$2\leqslant b<n$. 因为 a，b 是 n 的前导，所以它们都是素数或者是素数的乘积：

⊖ 定理 1.2 和定理 1.13 的证明类似，这表明第二归纳法仅仅是最小反例的一种变化形式.

$$a = pp'p''\cdots,\quad b = qq'q''\cdots,$$

因此 $n=pp'p''\cdots qq'q''\cdots$ 是素数(至少两个)的乘积. ■

这里用第二归纳法更方便，其原因是利用 $S(a)$ 和 $S(b)$ 比利用 $S(n-1)$ 更自然些. 事实上，根本不知道如何利用 $S(n-1)$.

这里有一个关于记号的说明. 我们改述第一归纳法中的归纳步骤：若 $S(n-1)$ 成立，则 $S(n)$ 成立(我们仍然说，若一个命题成立，则下一个命题成立). 这样，我们就可以比较两种形式的归纳法中的归纳步骤了. 两种形式都是想证明 $S(n)$：第一归纳法的归纳假设是 $S(n-1)$，第二归纳法的归纳假设是 $S(0)$，$S(1)$，…，$S(n-1)$ 中的任一个或所有的命题. 因此，看上去第二归纳法有一个更强的归纳假设. 而实际上，通过对习题 1.22 的证明，我们能发现数学归纳法的两种形式是等价的.

下面这一结果是说，我们可以从任何一个整数中分解出 2 的一个最大次幂来.

命题 1.14 每个整数 $n\geqslant 1$ 都有唯一分解 $n=2^k m$，其中 $k\geqslant 0$，$m\geqslant 1$ 是奇数.

证明 我们对 $n\geqslant 1$ 应用第二归纳法来证明 k 和 m 的存在性. 读者将看到这比使用第一归纳法更恰当.

基础步骤. 若 $n=1$，则取 $k=0$，$m=1$.

归纳步骤. 若 $n\geqslant 1$，则 n 是奇数或者是偶数. 当 n 是奇数时，取 $k=0$，$m=n$；当 n 是偶数时，取 $n=2b$. 因为 $b<n$，所以它是 n 的一个前导，归纳假设允许我们假设 $S(b)$: $b=2^{\ell}m$，其中 $\ell\geqslant 0$，m 是奇数. 这就得到了我们所希望的分解 $n=2b=2^{\ell+1}m$.

“唯一”指的是“恰有一个”. 为证明唯一性，我们需要证明：若 $n=2^k m=2^t m'$，其中 k 和 t 都是非负的，且 m 和 m' 都是奇数，则 $k=t$，$m=m'$. 不妨设 $k\geqslant t$. 假设 $k>t$，则从两边消去 2^t 得到 $2^{k-t}m=m'$. 由于 $k-t>0$，所以左边是偶数而右边是奇数，矛盾！因此 $k=t$. 我们再从两边消去 2^k 得到 $m=m'$. ■ 12

古希腊人认为这样的长方形最令人心情愉快：它的边 a 和 b 满足下述比例关系

$$a : b = b : (a+b).$$

于是 $a(a+b)=b^2$，所以 $b^2-ab-a^2=0$，即 $(b/a)^2-(b/a)-1=0$. 这个二次方程给出 $b/a=\frac{1}{2}(1\pm\sqrt{5})$. 因此，

$$b/a = \gamma = \frac{1}{2}(1+\sqrt{5})\quad \text{或}\quad b/a = \delta = \frac{1}{2}(1-\sqrt{5}).$$

γ 约等于 1.618 03，称之为**黄金比率**. 因为 γ 和 δ 是 x^2-x-1 的根，所以

$$\gamma^2 = \gamma + 1 \quad \text{和} \quad \delta^2 = \delta + 1.$$

我们讨论黄金比率的原因是：它和斐波那契序列密切相关.

定义 **斐波那契序列** F_0，F_1，F_2，…定义如下：

$$F_0 = 0, F_1 = 1, \text{对所有整数 } n \geqslant 2, F_n = F_{n-1} + F_{n-2}.$$

斐波那契序列是：0，1，1，2，3，5，8，13，….

命题 1.15 用 F_n 表示斐波那契序列的第 n 项，则对所有 $n\geqslant 0$ 有

$$F_n = \frac{1}{\sqrt{5}}(\gamma^n - \delta^n),$$

其中 $\gamma=\frac{1}{2}(1+\sqrt{5})$，$\delta=\frac{1}{2}(1-\sqrt{5})$.

证明 我们将用第二归纳法证明它[这里用第二归纳法是恰当的，因为方程 $F_n=F_{n-1}+F_{n-2}$表明，证明 $S(n)$既要用到 $S(n-1)$又要用到 $S(n-2)$].

基础步骤. 公式对 $n=0$ 成立：$\frac{1}{\sqrt{5}}(\gamma^0-\delta^0)=0=F_0$. 公式对 $n=1$ 也成立：

$$\begin{aligned}\frac{1}{\sqrt{5}}(\gamma^1-\delta^1)&=\frac{1}{\sqrt{5}}(\gamma-\delta)\\&=\frac{1}{\sqrt{5}}\left[\frac{1}{2}(1+\sqrt{5})-\frac{1}{2}(1-\sqrt{5})\right]\\&=\frac{1}{\sqrt{5}}(\sqrt{5})=1=F_1.\end{aligned}$$

[因为在证明关于 F_n 的归纳假设时需要用到关于 F_{n-1}和 F_{n-2}的命题的真实性，所以我们提到
13 了 $n=0$ 和 $n=1$. 例如，仅仅知道 $F_2=\frac{1}{\sqrt{5}}(\gamma^2-\delta^2)$不足以证明关于 F_3 的公式是正确的，我们还需要关于 F_1 的公式.]

归纳步骤. 若 $n\geqslant 2$，注意 $\gamma+1=\gamma^2$，$\delta+1=\delta^2$，则

$$\begin{aligned}F_n&=F_{n-1}+F_{n-2}\\&=\frac{1}{\sqrt{5}}(\gamma^{n-1}-\delta^{n-1})+\frac{1}{\sqrt{5}}(\gamma^{n-2}-\delta^{n-2})\\&=\frac{1}{\sqrt{5}}[(\gamma^{n-1}+\gamma^{n-2})-(\delta^{n-1}+\delta^{n-2})]\\&=\frac{1}{\sqrt{5}}[\gamma^{n-2}(\gamma+1)-\delta^{n-2}(\delta+1)]\\&=\frac{1}{\sqrt{5}}[\gamma^{n-2}(\gamma^2)-\delta^{n-2}(\delta^2)]\\&=\frac{1}{\sqrt{5}}(\gamma^n-\delta^n).\end{aligned}$$ ■

令人惊奇的是，整数 F_n 可以用无理数$\sqrt{5}$的关系式来表示.

推论 1.16 若 $\gamma=\frac{1}{2}(1+\sqrt{5})$，则对所有整数 $n\geqslant 3$ 有 $F_n>\gamma^{n-2}$.

注 若 $n=2$，则 $F_2=1=\gamma^0$，此时这是等式而不是不等式.

证明 基础步骤. 若 $n=3$，则 $F_3=2>\gamma$，因为 $\gamma\approx 1.618$.

归纳步骤. 我们必须证明 $F_{n+1}>\gamma^{n-1}$. 根据归纳假设，有

$$F_{n+1}=F_n+F_{n-1}>\gamma^{n-2}+\gamma^{n-3}=\gamma^{n-3}(\gamma+1)=\gamma^{n-3}\gamma^2=\gamma^{n-1}.$$ ■

我们也可以利用归纳法给出一些定义. 例如，可以对 $n\geqslant 0$ 用归纳法定义 n **的阶乘**,⊖记为 $n!$. 定义 $0!=1$，若 $n!$ 已知，则定义

⊖ 术语“因子”(factor)在拉丁文中指“构成”或“起作用”的意思；这样，术语“阶乘”(factorial)使人想到 $n!$ 有许多个因子.

$$(n+1)!=n!(n+1).$$

在下一节将会明显看到为什么要定义 $0!=1$.

习题

H 1.1　判断对错并说明理由.

(i)由负整数构成的每个非空集合中有一个最大整数.

(ii)存在一个由 13 个连续自然数构成的序列，其中恰有 2 个素数. 14

(iii)由 7 个连续自然数构成的任意序列中至少有两个素数.

(iv)在不含有 2 个素数的连续自然数构成的所有序列中，有一个序列的长度最短.

(v)79 是素数.

(vi)存在一组命题 $S(1)$，$S(2)$，…，满足 $S(2n)$ 对所有 $n\geqslant 1$ 都成立，而 $S(2n-1)$ 对所有 $n\geqslant 1$ 都不成立.

(vii)对所有 $n\geqslant 0$ 有 $n\leqslant F_n$，其中 F_n 是第 n 个斐波那契数.

(viii)若 m，n 都是自然数，则 $(mn)!=m!n!$.

*1.2　(i)对任意 $n\geqslant 0$ 和任意 $r\neq 1$，证明

$$1+r+r^2+r^3+\cdots+r^n=(1-r^{n+1})/(1-r).$$

H (ii)证明

$$1+2+2^2+\cdots+2^n=2^{n+1}-1.$$

H 1.3　证明对所有 $n\geqslant 1$，10^n 被 9 除后余数是 1.

1.4　试证：若 $0\leqslant a\leqslant b$，则对所有 $n\geqslant 0$ 有 $a^n\leqslant b^n$.

1.5　试证 $1^2+2^2+\cdots+n^2=\frac{1}{6}n(n+1)(2n+1)=\frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$.

1.6　试证 $1^3+2^3+\cdots+n^3=\frac{1}{4}n^4+\frac{1}{2}n^3+\frac{1}{4}n^2$.

1.7　试证 $1^4+2^4+\cdots+n^4=\frac{1}{5}n^5+\frac{1}{2}n^4+\frac{1}{3}n^3-\frac{1}{30}n$.

H 1.8　求 $1+3+5+\cdots+(2n-1)$ 的计算公式，并用数学归纳法加以证明.（在数学中用归纳推理有助于猜测什么可能成立，一旦作出了猜测，我们还要对猜测进行证明，或用数学归纳法，或用其他方法.）

H 1.9　求 $1+\sum_{j=1}^{n}j!j$ 的计算公式，并用数学归纳法加以证明.

1.10　(**M. Barr**) 有一件著名的轶事，描述了哈代(G. H. Hardy)去医院看望拉马努金(Ramanujan)的情况. 哈代提到他来医院所乘坐的出租车的号码 1729 不是一个令人感兴趣的数字，而拉马努金不同意这个看法，说这个数是可以用两种方法写成两个立方数的和的最小正整数.

(i)证明拉马努金的陈述是对的.

H (ii)证明拉马努金的陈述是错的.

***H** 1.11　通过利用图 1-1 计算边长为 $n+1$ 的正方形的面积 $(n+1)^2$，导出 $\sum_{i=1}^{n}i$ 的计算公式.

*1.12　**H** (i)通过计算如图 1-2 所示的底为 n 高为 $n+1$ 的长方形的面积 $n(n+1)$，导出 $\sum_{i=1}^{n}i$ 的计算公式.

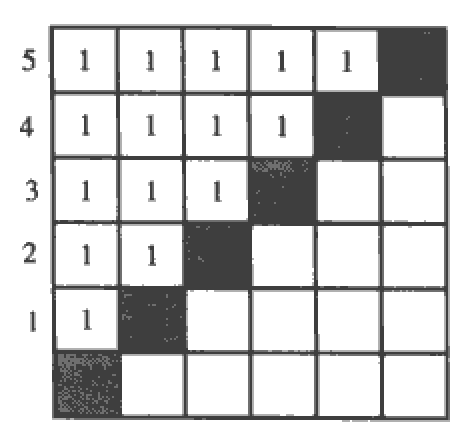


图 1-1　$1+2+\cdots+n=\frac{1}{2}(n^2+n)$

H (ii)(**阿尔哈曾(Alhazen)公式**)对固定的 $k\geqslant 1$，利用图 1-3 证明

$$(n+1)\sum_{i=1}^{n} i^k = \sum_{i=1}^{n} i^{k+1} + \sum_{i=1}^{n}\Big(\sum_{p=1}^{i} p^k\Big).$$

H (iii)给定公式 $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$，利用(ii) 导出 $\sum_{i=1}^{n} i^2$ 的计算公式.

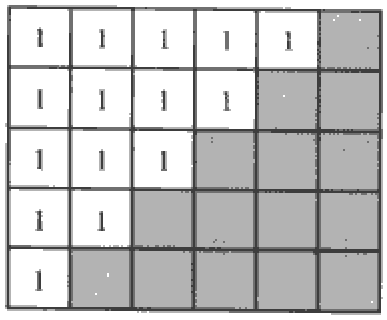


图 1-2 $1+2+\cdots+n=\frac{1}{2}n(n+1)$

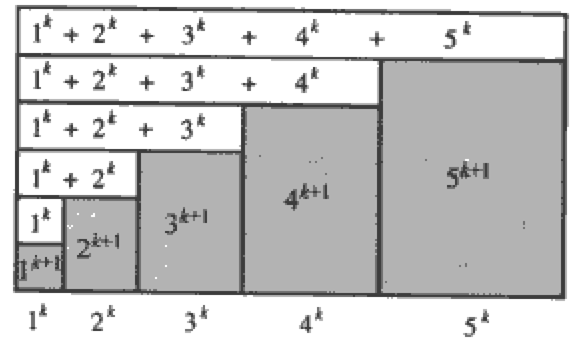


图 1-3 阿尔哈曾的分割

1.13 **H** (i)证明对所有 $n\geqslant 10$，有 $2^n>n^3$.

15 **H** (ii)证明对所有 $n\geqslant 17$，有 $2^n>n^4$.

H 1.14 大约在 1350 年，奥雷姆(N. Oresme)就能通过图 1-4 中的分割用两种方法求级数 $\sum_{n=1}^{\infty} n/2^n$ 的和. 设 A_n 是底为 $\frac{1}{2^n}$ 高为 n 的直角三角形，其面积为 $\text{area}(A_n)=n/2^n$，再设 B_n 是底为 $\frac{1}{2^n}+\frac{1}{2^{n+1}}+\cdots$ 高为 1 的矩形. 证明 $\sum_{n=1}^{\infty} n/2^n=2$.

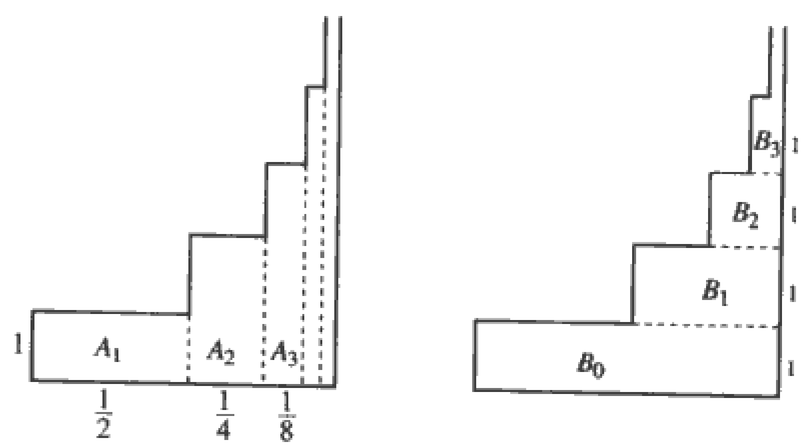


图 1-4 奥雷姆的分割

***H** 1.15 设 $g_1(x)$，…，$g_n(x)$都是可微函数，$f(x)$是它们的积：$f(x)=g_1(x)\cdots g_n(x)$. 证明：对所有整数 $n\geqslant 2$ 有

$$f'(x)=\sum_{i=1}^{n} g_1(x)\cdots g_{i-1}(x)g_i'(x)g_{i+1}(x)\cdots g_n(x).$$

H 1.16 证明：对每个 $n\in\mathbb{N}$，只要 $x\in\mathbb{R}$ 且 $1+x>0$ 就有$(1+x)^n\geqslant 1+nx$.

16 **H** 1.17 证明：每个正整数 a 有唯一的分解式 $a=3^k m$，其中 $k\geqslant 0$，m 不是 3 的倍数.

H 1.18 证明：对所有 $n\geqslant 0$ 有 $F_n<2^n$，其中 F_0，F_1，F_2，…都是斐波那契序列.

H 1.19 若 F_n 表示斐波那契序列中的第 n 项，证明

$$\sum_{n=1}^{m} F_n = F_{m+2}-1.$$

H 1.20　证明：对所有 $n\geqslant 1$，$4^{n+1}+5^{2n-1}$能被 21 整除.

H 1.21　对任意整数 $n\geqslant 2$，证明存在 n 个相邻的合数. 由此得出相邻素数之间的间距可以任意大.

*1.22　证明第一数学归纳法和第二数学归纳法是等价的，即证明定理 1.4 成立当且仅当定理 1.12 成立.

*1.23　（**双归纳法**）对每个 $m\geqslant 0$ 和 $n\geqslant 0$，设 $S(m, n)$是一组双指标命题. 假设

(i)$S(0, 0)$成立；

(ii)若 $S(m, 0)$成立，则 $S(m+1, 0)$成立；

(iii)若 $S(m, n)$对所有 $m\geqslant 0$ 成立，则 $S(m, n+1)$对所有 $m\geqslant 0$ 成立.

证明：对所有 $m\geqslant 0$ 和 $n\geqslant 0$，$S(m, n)$成立.

1.24　用双归纳法证明对所有 $m, n\geqslant 0$ 有

$$(m+1)^n > mn.$$

H 1.25　对每个锐角 θ，即 $0°<\theta<90°$，证明

$$\sin\theta+\cot\theta+\sec\theta\geqslant 3.$$

*1.26　H (i)设 p 是一个正数. 若△是一个等边三角形，周长 $p=2s$，证明 $\text{area}(\triangle)=s^2/\sqrt{27}$.

H (ii)证明：在平面上周长为 p 的所有三角形中等边三角形的面积最大. 17

H 1.27　证明：若 $a_1, a_2, \cdots, a_n$ 都是正数，则

$$(a_1+a_2+\cdots+a_n)(1/a_1+1/a_2+\cdots+1/a_n)\geqslant n^2.$$

→1.2　二项式定理与复数

二项式 $1+x$ 的幂$(1+x)^n$展开式中的系数具有何种形式呢？前面的几个展开式是：

$$(1+x)^0=1$$
$$(1+x)^1=1+1x$$
$$(1+x)^2=1+2x+1x^2$$
$$(1+x)^3=1+3x+3x^2+1x^3$$
$$(1+x)^4=1+4x+6x^2+4x^3+1x^4.$$

图 1-5 称为**帕斯卡三角形**，这是帕斯卡(B. Pascal，1623—1662)给出的前面几个展开式的系数排列. 图 1-6 是 1303 年出自中国的一幅图，它表明早在帕斯卡出生前关于二项式系数的形式就已经被发现了.

1
1　1
1　2　1
1　3　3　1
1　4　6　4　1
1　5　10　10　5　1
1　6　15　20　15　6　1
1　7　21　35　35　21　7　1

图　1-5

$(1+x)^n$的展开式如下： 18

$$c_0+c_1x+c_2x^2+\cdots+c_nx^n.$$

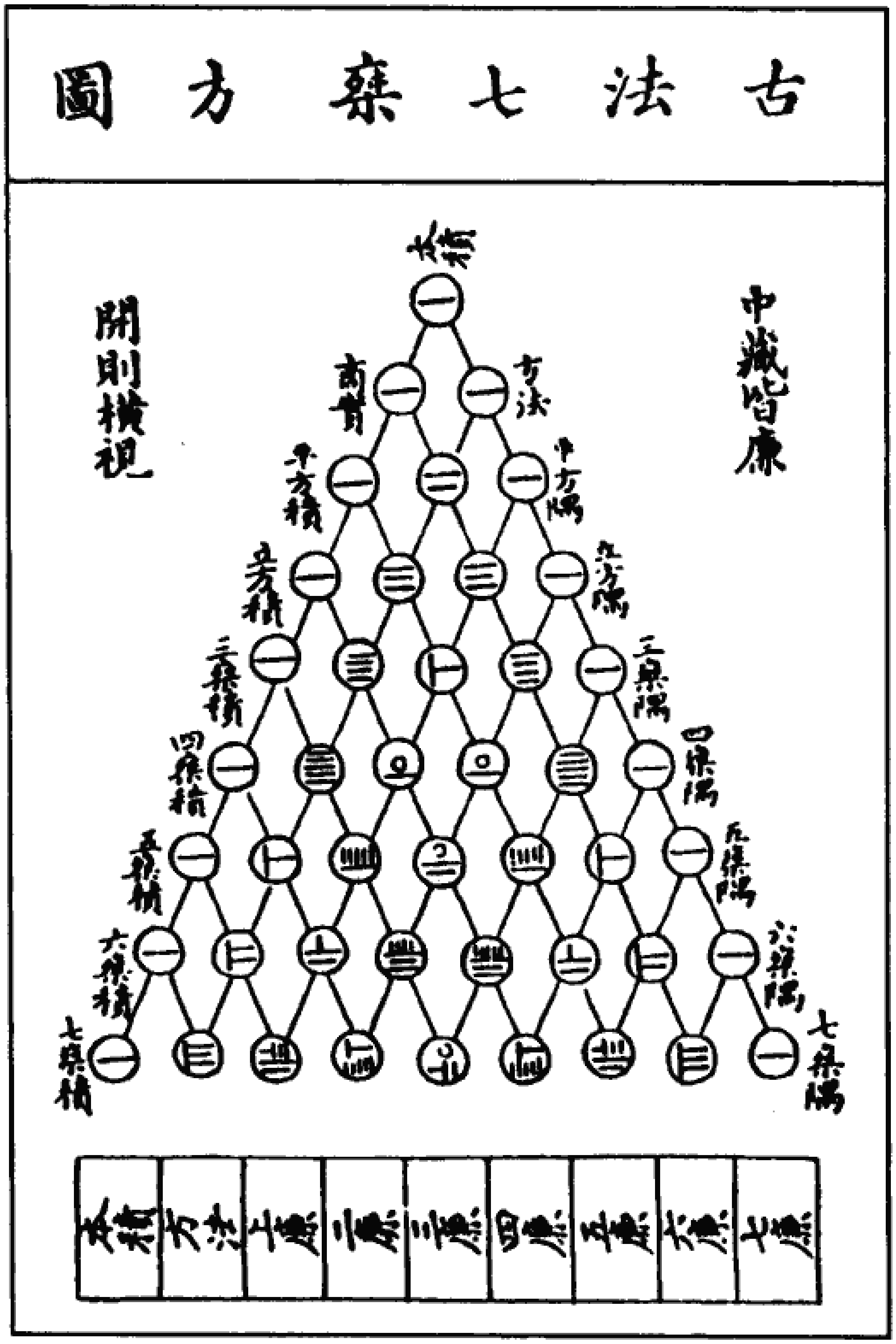
系数 c_r 称为**二项式系数**⊖. 欧拉(L. Euler，1707—1783)曾引用符号$\left(\frac{n}{r}\right)$来表示二项式系数，这个符号后来演变成现在普遍采用的符号：

⊖ "二项式"(binomial)来自拉丁文中意指"两个"的 bi 和意指"姓名"或"术语"的 nomen，描述了形如 $a+b$ 的表达式. 类似地，"三项式"(trinomial)描述了形如 $a+b+c$ 的表达式，"单项式"(monomial)描述了只有一个单项的表达式. 使用这个单词是因为：当扩大二项式 $1+x$ 的幂时会出现二项式系数. "多项式"(polynomial)是一个合成词，来自希腊文中意指"许多"的 poly 和拉丁文中的 nomen. 多项式是指含有许多项的表达式.

$$\binom{n}{r} = (1+x)^n \text{ 中 } x^r \text{ 的系数 } c_r.$$

这样，

$$(1+x)^n = \sum_{r=0}^{n} \binom{n}{r} x^r.$$



19 图 1-6 帕斯卡三角形源于中国，1300 年

因为 $\binom{n}{r}$ 是在计数问题中产生的，所以它读作“n 个中选 r 个”，关于这个内容我们将在本

节后面的部分看到.

观察图 1-5 可知，第$(n+1)$行中每个除 1 之外的数都可以由第 n 行中位于其肩上的两个数相加得到. 例如，第四行中除 1 之外的数都可由第三行

$$\begin{matrix} & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{matrix}$$

中的数按如下方法得到：$4=1+3$，$6=3+3$，$4=3+1$. 现在我们来证明这种观察是对的.

→ **引理 1.17** 对所有整数 $n\geqslant 1$ 和所有满足 $0<r<n+1$ 的 r，有

$$\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$$

证明 我们必须证明，对所有 $n\geqslant 1$，若

$$(1+x)^n=c_0+c_1x+c_2x^2+\cdots+c_nx^n,$$ 20

则$(1+x)^{n+1}$中 x^r 的系数是 $c_{r-1}+c_r$. 由于 $c_0=1$，

$$\begin{aligned}(1+x)^{n+1}&=(1+x)(1+x)^n\\&=(1+x)^n+x(1+x)^n\\&=(c_0+c_1x+c_2x^2+\cdots+c_nx^n)+x(c_0+c_1x+c_2x^2+\cdots+c_nx^n)\\&=(c_0+c_1x+c_2x^2+\cdots+c_nx^n)+c_0x+c_1x^2+c_2x^3+\cdots+c_nx^{n+1}\\&=1+(c_0+c_1)x+(c_1+c_2)x^2+(c_2+c_3)x^3+\cdots.\end{aligned}$$

因此$(1+x)^{n+1}$中 x^r 的系数$\binom{n+1}{r}$是

$$c_{r-1}+c_r=\binom{n}{r-1}+\binom{n}{r}.$$ ■

→ **命题 1.18（帕斯卡）** 对所有 $n\geqslant 0$ 和所有 r，$0\leqslant r\leqslant n$，有

$$\binom{n}{r}=\frac{n!}{r!(n-r)!}.$$

证明 对 $n\geqslant 0$ 用归纳法证之.

基础步骤.[⊖]若 $n=0$，则$\binom{0}{0}=\frac{0!}{0!\ 0!}=1$.

归纳步骤. 假设对所有 r，公式都对$\binom{n}{r}$成立，我们必须证明

$$\binom{n+1}{r}=\frac{(n+1)!}{r!(n+1-r)!}.$$

若 $r=0$，则$\binom{n+1}{0}=1=\frac{(n+1)!}{0!(n+1-0)!}$；若 $r=n+1$，则$\binom{n+1}{n+1}=1=\frac{(n+1)!}{(n+1)!0!}$；若 $0<r<$ 21
$n+1$，利用引理 1.17 有

⊖ 这是定义 $0!=1$ 的原因之一.

$$\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$$
$$=\frac{n!}{(r-1)!(n-r+1)!}+\frac{n!}{r!(n-r)!}$$
$$=\frac{n!}{(r-1)!(n-r)!}\left(\frac{1}{(n-r+1)}+\frac{1}{r}\right)$$
$$=\frac{n!}{(r-1)!(n-r)!}\left(\frac{r+n-r+1}{r(n-r+1)}\right)$$
$$=\frac{n!}{(r-1)!(n-r)!}\left(\frac{n+1}{r(n-r+1)}\right)$$
$$=\frac{(n+1)!}{r!(n+1-r)!}.$$ ■

推论 1.19 对所有实数 x 和所有整数 $n\geqslant 0$，有

$$(1+x)^n=\sum_{r=0}^{n}\binom{n}{r}x^r=\sum_{r=0}^{n}\frac{n!}{r!(n-r)!}x^r.$$

证明 第一个等式是二项式系数的定义，第二个等式可用帕斯卡定理所给的值代替 $\binom{n}{r}$ 得到. ■

→ **推论 1.20（二项式定理）** 对所有实数 a，b 和所有整数 $n\geqslant 1$，有

$$(a+b)^n=\sum_{r=0}^{n}\binom{n}{r}a^{n-r}b^r=\sum_{r=0}^{n}\left(\frac{n!}{r!(n-r)!}\right)a^{n-r}b^r.$$

证明 当 $a=0$ 时，结论显然是成立的（如果我们约定 $0^0=1$）. 当 $a\neq 0$ 时，在推论 1.19 中令 $x=b/a$，并观察

$$\left(1+\frac{b}{a}\right)^n=\left(\frac{a+b}{a}\right)^n=\frac{(a+b)^n}{a^n}.$$

因此，

22 $$(a+b)^n=a^n\left(1+\frac{b}{a}\right)^n=a^n\sum_{r=0}^{n}\binom{n}{r}\frac{b^r}{a^r}=\sum_{r=0}^{n}\binom{n}{r}a^{n-r}b^r.$$ ■

注 二项式定理可放在推论 1.19 之前证明，即只需对 $n\geqslant 0$ 用归纳法证明 $(a+b)^n$ 的展开式. 我们选择上面的证明方法是为了使证明看起来更清楚.

以下是对二项式系数在组合论中的解释. 给定一个集合 X，一个 **r-子集**是指恰含 r 个元素的 X 的子集. 若 X 有 n 个元素，则它的 r-子集的个数记作

$$[n,r],$$

即 $[n,r]$ 是从盛有 n 个物体的盒子里选出 r 个物体的方法数.

我们通过考虑一个相关的问题来计算 $[n,r]$ 的值. 给定一个含有 n 个互异字母的“字母表”以及整数 $r(1\leqslant r\leqslant n)$，一个 **$r$-变位字**是指 r 个不重复的字母构成的序列. 例如，字母表 a，b，c 中的 2-变位字是

$$ab,ba,ac,ca,bc,cb$$

(注意 aa，bb，cc 不在这个序列中). 含 n 个字母的字母表中的 r-变位字有多少个呢？我们用两种方法来计算：

(1)第一个字母有 n 种选法，由于字母不重复，所以第二个字母只有 $n-1$ 种选法，第三个字母只有 $n-2$ 种，依此类推. 因此 r-变位字的个数是

$$n(n-1)(n-2)\cdots(n-[r-1]) = n(n-1)(n-2)\cdots(n-r+1).$$

注意特殊情形 $n=r$：n-变位字的个数是 $n!$.

(2)第二种计算方法. 首先选取字母表的一个 r-子集(由 r 个字母构成)，因为这正是符号 $[n,r]$的含义，所以有$[n,r]$种选取方法. 对每个选出的 r-子集，有 $r!$ 种方法排列这 r 个字母(这是(1)的特殊情形 $n=r$). 因此 r-变位字的个数是

$$r![n,r].$$

我们得到

$$r![n,r] = n(n-1)(n-2)\cdots(n-r+1),$$

于是，根据帕斯卡定理，有

$$[n,r] = n(n-1)(n-2)\cdots(n-r+1)/r! = \binom{n}{r}.$$

这个事实正是人们经常把二项式系数 $\binom{n}{r}$ 读作"n 个中选 r 个"的原因.

例如，从放有 14 顶不同帽子的抽屉中选出 2 顶帽子来，有多少种方法呢？(我的一个朋友不喜欢这个问题的提法，毕竟人们可以用自己的左手或右手或牙齿等等来选出 2 顶帽子，但我 [23]
继续这个提法.)回答是 $\binom{14}{2}$，且用帕斯卡定理计算得$(14\times13)/2=91$.

我们对二项式系数 $\binom{n}{r}$ 的第一种解释属于代数学方面，也就是说，把它看作可用帕斯卡定理计算的多项式的系数. 第二种解释属于组合论方面，即 n 个中选 r 个. 通常，每种解释都可以用来证明一个我们所希望的结果. 例如，下面是引理 1.17 在组合论中的一个证明. 设 X 是一个含有 $n+1$ 个元素的集合，我们将其中一个元素染成红色，其他 n 个元素都染成蓝色，则 $\binom{n+1}{r}$ 等于 X 的 r-子集的个数. 对一个 r-子集 Y 有两种可能：或者它含有红色元素或者它的元素全是蓝色的. 若 Y 含有红色元素，则 Y 由一个红色元素和 $r-1$ 个蓝色元素构成，此时这样的 Y 的个数与所有蓝色$(r-1)$-子集的个数相等，都为 $\binom{n}{r-1}$ 个. 另一种可能是 Y 中的元素都是蓝色的，此时有 $\binom{n}{r}$ 个这样的 r-子集. 因此 $\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$，这正是我们所希望的.

现在我们把二项式定理应用到三角学中去，但是先回顾一下复数的有关性质. 回忆一下，一个复数 $z=a+ib$ 的模 $|z|$ 被定义为

$$|z| = \sqrt{a^2+b^2}.$$

如果我们把一个复数 $z=a+ib$ 与平面上的一个点 (a, b) 等同起来，则它的模 $|z|$ 就是 z 与原点的距离. 于是模为 1 的复数 z 对应着单位圆上的点 P（见图 1-7）. 在右边的三角形 OPA 中，因为 $|OP|=1$，所以 $\cos\theta=|OA|/|OP|=|OA|$，$\sin\theta=|PA|/|OP|=|PA|$. 因此点 P 的坐标为 $(\cos\theta, \sin\theta)$.

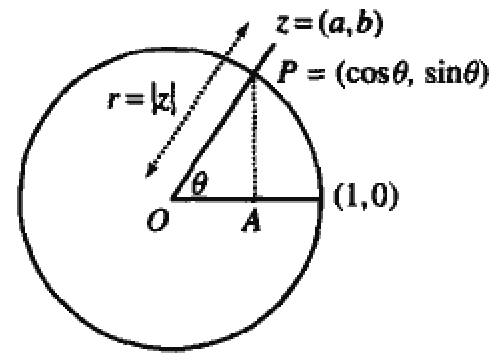


图 1-7 $(a, b)=r(\cos\theta+i\sin\theta)$

这里有求非零复数的逆元的一种最简方法. 若 $z=a+ib$，其中 a 和 b 都是实数，则定义它的**复共轭**为 $\bar{z}=a-ib$. 注意到 $z\bar{z}=a^2+b^2$，所以 $z\neq 0$ 当且仅当 $z\bar{z}\neq 0$. 若 $z\neq 0$ 则

24 $$z^{-1}=1/z=\bar{z}/z\bar{z}=(a/z\bar{z})-i(b/z\bar{z}).$$

于是，若 z 位于单位圆上则 z^{-1} 也位于单位圆上，而且此时有 $z^{-1}=\bar{z}$. 读者可以验证下列几个等式对所有复数 z 和 w 都成立：

$$\overline{z+w}=\bar{z}+\bar{w}$$

$$\overline{zw}=\bar{z}\,\bar{w}$$

$$\bar{\bar{z}}=z.$$

而且，$\bar{z}=z$ 当且仅当 z 是一个实数.

→ **命题 1.21（极分解定理）** *对每个复数 z，都存在一个分解*

$$z=r(\cos\theta+i\sin\theta),$$

其中 $r=|z|\geqslant 0$，$0\leqslant\theta<2\pi$.

证明 若 $z=0$，则 $|z|=0$，θ 可以任意选取. 若 $z=a+bi\neq 0$，则 $|z|\neq 0$. 因为 $(a/|z|)^2+(b/|z|)^2=(a^2+b^2)/|z|^2=1$，所以 $z/|z|=a/|z|+ib/|z|$ 的模为 1. 因此存在一个角 θ 满足

$$\frac{z}{|z|}=\cos\theta+i\sin\theta,$$

因而 $z=|z|(\cos\theta+i\sin\theta)=r(\cos\theta+i\sin\theta)$. ∎

若 $z=a+ib=r(\cos\theta+i\sin\theta)$，则 (r, θ) 称为 z 的**极坐标**[⊖]，这就是命题 1.21 称为 z 的极分解的原因.

关于 $\cos(\theta+\psi)$ 和 $\sin(\theta+\psi)$ 的三角加法公式在复数语言中有一个可爱的翻译.

命题 1.22（加法定理） *若*

$$z=\cos\theta+i\sin\theta,\quad w=\cos\psi+i\sin\psi,$$

则

$$zw=\cos(\theta+\psi)+i\sin(\theta+\psi).$$

证明

$$zw=(\cos\theta+i\sin\theta)(\cos\psi+i\sin\psi)$$

25 $$=(\cos\theta\cos\psi-\sin\theta\sin\psi)+i(\sin\theta\cos\psi+\cos\theta\sin\psi).$$

⊖ "极(pole)"是指一根轴，旋转是围绕它产生的. 例如，地球的轴有端点北极和南极. 这里，我们取极为 z 轴（垂直于平面）.

由三角加法公式知

$$zw = \cos(\theta+\psi) + \mathrm{i}\sin(\theta+\psi).$$ ■

加法定理给出了复数乘法的一个几何解释：若 $z=r(\cos\theta+\mathrm{i}\sin\theta)$，$w=s(\cos\psi+\mathrm{i}\sin\psi)$，则

$$zw = rs[\cos(\theta+\psi) + \mathrm{i}\sin(\theta+\psi)],$$

且 zw 的极坐标是

$$(rs, \theta+\psi).$$

→ **推论 1.23** 若 z，w 是复数，则

$$|zw| = |z||w|.$$

证明 若 z 和 w 的极分解分别是 $z=r(\cos\theta+\mathrm{i}\sin\theta)$ 和 $w=s(\cos\psi+\mathrm{i}\sin\psi)$，则如刚才所看到的，有 $|z|=r$，$|w|=s$，$|zw|=rs$. ■

由这个推论可知，若 z 和 w 都位于单位圆上，则它们的乘积 zw 也位于单位圆上.

在 1707 年，棣莫弗(A. De Moivre，1667—1754)证明了下面一个优美的结论.

定理 1.24 (棣莫弗) 对每个实数 x 和每个正整数 n 有

$$\cos(nx) + \mathrm{i}\sin(nx) = (\cos x + \mathrm{i}\sin x)^n.$$

证明 我们对 $n\geqslant 1$ 用归纳法证明棣莫弗定理. 基础步骤 $n=1$ 时，结论显然是成立的. 对归纳步骤，有

$$\begin{aligned}(\cos x + \mathrm{i}\sin x)^{n+1} &= (\cos x + \mathrm{i}\sin x)^n(\cos x + \mathrm{i}\sin x)\\ &= [\cos(nx) + \mathrm{i}\sin(nx)](\cos x + \mathrm{i}\sin x) \quad (\text{归纳假设})\\ &= \cos(nx + x) + \mathrm{i}\sin(nx + x) \quad (\text{加法公式})\\ &= \cos([n+1]x) + \mathrm{i}\sin([n+1]x).\end{aligned}$$ ■

例 1.25 求 $(\cos 3^\circ + \mathrm{i}\sin 3^\circ)^{40}$ 的值. 根据棣莫弗定理有

$$(\cos 3^\circ + \mathrm{i}\sin 3^\circ)^{40} = \cos 120^\circ + \mathrm{i}\sin 120^\circ = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}.$$ ◀

以下是二倍角和三倍角公式. 26

推论 1.26

(i) $\cos(2x) = \cos^2 x - \sin^2 x = 2\cos^2 x - 1$

$\sin(2x) = 2\sin x\cos x.$

(ii) $\cos(3x) = \cos^3 x - 3\cos x\sin^2 x = 4\cos^3 x - 3\cos x$

$\sin(3x) = 3\cos^2 x\sin x - \sin^3 x = 3\sin x - 4\sin^3 x.$

证明 (i) 由棣莫弗定理知

$$\begin{aligned}\cos(2x) + \mathrm{i}\sin(2x) &= (\cos x + \mathrm{i}\sin x)^2\\ &= \cos^2 x + 2\mathrm{i}\sin x\cos x + \mathrm{i}^2\sin^2 x\\ &= \cos^2 x - \sin^2 x + \mathrm{i}(2\sin x\cos x).\end{aligned}$$

让两边的实部和虚部分别相等，得到倍角公式.

(ii)由棣莫弗定理知

$$\begin{aligned}\cos(3x)+\mathrm{i}\sin(3x)&=(\cos x+\mathrm{i}\sin x)^3\\&=\cos^3x+3\mathrm{i}\cos^2x\sin x+3\mathrm{i}^2\cos x\sin^2x+\mathrm{i}^3\sin^3x\\&=\cos^3x-3\cos x\sin^2x+\mathrm{i}(3\cos^2x\sin x-\sin^3x).\end{aligned}$$

由实部相等得 $\cos(3x)=\cos^3x-3\cos x\sin^2x$，用 $1-\cos^2x$ 代替 $\sin^2x$ 可得第一个公式. 由虚部相等得 $\sin(3x)=3\cos^2x\sin x-\sin^3x=3\sin x-4\sin^3x$，用 $1-\sin^2x$ 代替 $\cos^2x$ 可得第二个公式. ■

推论 1.26 可以在命题 1.27 中得到推广. 若 $f_2(x)=2x^2-1$，则

$$\cos(2x)=2\cos^2x-1=f_2(\cos x),$$

若 $f_3(x)=4x^3-3x$，则

$$\cos(3x)=4\cos^3x-3\cos x=f_3(\cos x).$$

命题 1.27 *对所有 $n\geqslant1$，存在一个整系数多项式 $f_n(x)$ 满足*

$$\cos(nx)=f_n(\cos x).$$

证明 根据棣莫弗定理有

27

$$\begin{aligned}\cos(nx)+\mathrm{i}\sin(nx)&=(\cos x+\mathrm{i}\sin x)^n\\&=\sum_{r=0}^{n}\binom{n}{r}(\cos x)^{n-r}(\mathrm{i}\sin x)^r.\end{aligned}$$

左边的实部 $\cos(nx)$ 必须等于右边的实部. i^r 是实数当且仅当[㊀] r 是偶数，所以

$$\cos(nx)=\sum_{r\,\text{偶数}}^{n}\binom{n}{r}(\cos x)^{n-r}(\mathrm{i}\sin x)^r.$$

若 $r=2k$，则 $\mathrm{i}^r=\mathrm{i}^{2k}=(-1)^k$，且

$$\cos(nx)=\sum_{k=0}^{\lfloor n/2\rfloor}(-1)^k\binom{n}{2k}(\cos x)^{n-2k}\sin^{2k}x.$$

($\lfloor n/2\rfloor$ 表示满足 $m\leqslant n/2$ 的最大整数 m)[㊁]. 但是 $\sin^{2k}x=(\sin^2x)^k=(1-\cos^2x)^k$，这正是 $\cos x$ 的一个多项式，证明完毕. ■

不难证明 $f_n(x)$ 的第一项是 $2^{n-1}x^n$. 命题 1.27 的正弦公式可以在习题 1.37 中找到.

我们下面将要给出欧拉(Euler)发现的一个漂亮公式，先回忆一下微积分学中的一些幂级数公式，以便看出该公式是如何产生的. 对每个实数 x，

$$\mathrm{e}^x=1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}+\cdots,$$

$$\cos x=1-\frac{x^2}{2!}+\frac{x^4}{4!}-\cdots+\frac{(-1)^nx^{2n}}{(2n)!}+\cdots,$$

和

$$\sin x=x-\frac{x^3}{3!}+\frac{x^5}{5!}-\cdots+\frac{(-1)^nx^{2n+1}}{(2n+1)!}+\cdots.$$

㊀ 命题"若 P 真则 Q 真"的逆命题是"若 Q 真则 P 真". 一个命题成立但它的逆命题可能不成立. 例如，命题"若 $a=b$ 则 $a^2=b^2$". 短语"当且仅当"是指命题及其逆命题都成立.

㊁ $\lfloor x\rfloor$ 表示满足 $m\leqslant x$ 的最大整数 m，读作 x 的下取整或 x 中的最大整数. 例如，$\lfloor 3\rfloor=3$ 和 $\lfloor \pi\rfloor=3$.

我们可以定义幂级数 $\sum_{n=0}^{\infty} c_n z^n$（$z$ 和 c_n 是复数）的收敛性，并且可以证明级数

$$1+z+\frac{z^2}{2!}+\cdots+\frac{z^n}{n!}+\cdots$$

对每个复数 z 都收敛，我们定义该级数的和为**复指数** e^z. 28

欧拉定理　对所有实数 x，有

$$e^{ix}=\cos x+i\sin x.$$

证明（简要证明）　现在

$$e^{ix}=1+ix+\frac{(ix)^2}{2!}+\cdots+\frac{(ix)^n}{n!}+\cdots.$$

当 n 取值 0，1，2，3，…时，i 的 n 次幂每四步重复一次：即 i^n 取值

$$1,i,-1,-i,1,i,-1,-i,1,\cdots.$$

于是，ix 的偶次幂不含 i 而奇次幂含有 i. 合并所有项，我们有 e^{ix}＝偶次项＋奇次项，其中

$$\begin{aligned}\text{偶次项}&=1+\frac{(ix)^2}{2!}+\frac{(ix)^4}{4!}+\cdots\\&=1-\frac{x^2}{2!}+\frac{x^4}{4!}-\cdots=\cos x\\\text{奇次项}&=ix+\frac{(ix)^3}{3!}+\frac{(ix)^5}{5!}+\cdots\\&=i\left(x-\frac{x^3}{3!}+\frac{x^5}{5!}-\cdots\right)=i\sin x.\end{aligned}$$

因此 $e^{ix}=\cos x+i\sin x$. ∎

作为欧拉定理的一个结果，极分解定理可以被重新写为指数形式：每个复数 z 有分解

$$z=re^{i\theta},$$

其中 $r\geqslant 0$，$0\leqslant\theta<2\pi$.

加法定理和棣莫弗定理可以被重新写为复指数形式：第一个变为

$$e^{ix}e^{iy}=e^{i(x+y)};$$

第二个变为

$$(e^{ix})^n=e^{inx}.$$

→ **定义**　设 $n\geqslant 1$ 是整数，若复数 ζ 满足 $\zeta^n=1$，则 ζ 称为 n **次单位根**. 29

→ **推论 1.28**　每个 n 次单位根 ζ 等于

$$e^{2\pi ik/n}=\cos(2\pi k/n)+i\sin(2\pi k/n),$$

其中 $0\leqslant k\leqslant n-1$.

证明　若 $\zeta=\cos(2\pi/n)+i\sin(2\pi/n)$，则由棣莫弗定理即定理 1.24 得

$$\begin{aligned}\zeta^n&=[\cos(2\pi/n)+i\sin(2\pi/n)]^n\\&=\cos(n2\pi/n)+i\sin(n2\pi/n)\\&=\cos(2\pi)+i\sin(2\pi)\\&=1,\end{aligned}$$

所以 ζ 是一个 n 次单位根. 最后，若 k 是一个整数，则由 $\zeta^n=1$ 推出 $(\zeta^k)^n=(\zeta^n)^k=1^k=1$，所以 $\zeta^k=\cos(2\pi k/n)+\mathrm{i}\sin(2\pi k/n)$ 也是一个 n 次单位根.

反之，假设 ζ 是一个 n 次单位根. 根据极分解定理即命题 1.21，我们有 $\zeta=\cos\theta+\mathrm{i}\sin\theta$(因为 $|\zeta|=1$). 根据棣莫弗定理，有 $1=\zeta^n=\cos n\theta+\mathrm{i}\sin n\theta$. 因为 $\cos\theta=1$ 当且仅当 $\theta=2k\pi$，k 为整数，所以有 $n\theta=2k\pi$，即 $\zeta=\cos(2k\pi/n)+\mathrm{i}\sin(2k\pi/n)$. 显然，我们可以选取 k 使得 $0\leqslant k<n$，因为 $\cos x$ 是以 2π 为周期的周期函数. ■

推论 1.28 的充分性有一个更为代数化的证明. 我们将证明(定理 3.50)次数为 n 的多项式至多有 n 个根. 因为 n 个 n 次单位根即 $e^{2\pi ik/n}$，$k=0, 1, \cdots, n-1$，都是 x^n-1 的不同根，所以没有其他的 n 次单位根.

推论 1.23 是说，对任意复数 z 和 w 有 $|zw|=|z||w|$. 于是，若 ζ 是一个 n 次单位根，则 $1=|\zeta^n|=|\zeta|^n$，所以 $|\zeta|=1$，ζ 位于单位圆上. 给定一个正整数 n，设 $\theta=2\pi/n$，$\zeta=e^{i\theta}$. ζ 的极坐标是 $(1, \theta)$，ζ^2 的极坐标是 $(1, 2\theta)$，ζ^3 的极坐标是 $(1, 3\theta)$，ζ^{n-1} 的极坐标是 $(1, (n-1)\theta)$，$\zeta^n=1$ 的极坐标是 $(1, n\theta)=(1, 0)$. 因此 n 次单位根均匀地分布在单位圆上. 图 1-8 展示了 8 次单位根(这里 $\theta=2\pi/8=\pi/4$).

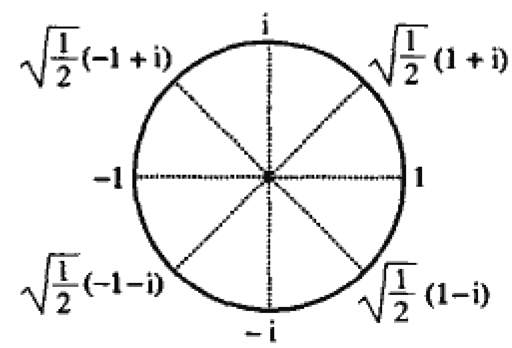


图 1-8 8 次单位根

像数 a 的平方根有 $\pm\sqrt{a}$ 一样，a 的不同的 n 次方根有 n 个，即 $e^{2\pi ik/n}\sqrt[n]{a}$，$k=0, 1, \cdots, n-1$. 例如，1 的立方根是 1，

$$\zeta=\cos 120^\circ+\mathrm{i}\sin 120^\circ=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$$

和

30 $$\zeta^2=\cos 240^\circ+\mathrm{i}\sin 240^\circ=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}.$$

2 的立方根有 3 个，即 $\sqrt[3]{2}$，$\zeta\sqrt[3]{2}$，$\zeta^2\sqrt[3]{2}$.

当然，每个 n 次单位根都是多项式 x^n-1 的一个根. 因此，

$$x^n-1=\prod_{\zeta^n=1}(x-\zeta).$$

若 ζ 是一个 n 次单位根，且 n 是满足 $\zeta^n=1$ 的最小正整数，则我们就说 ζ 是一个 **n 次本原单位根**. 例如，$\zeta=e^{2\pi i/n}$ 是一个 n 次本原单位根. 因为 $i^8=1$，所以 i 是一个 8 次单位根，它不是一个 8 次本原单位根，但是是一个 4 次本原单位根.

引理 1.29 *设 ζ 是一个 d 次本原单位根. 若 $\zeta^n=1$，则 d 一定是 n 的一个因子.*

证明 根据长除法有 $n/d=q+r/d$，其中 q，r 都是自然数，且 $0\leqslant r/d<1$，即 $n=qd+r$，其中 $0\leqslant r<d$. 但是，因为 $\zeta^{qd}=(\zeta^d)^q=1$，所以

$$1=\zeta^n=\zeta^{qd+r}=\zeta^{qd}\zeta^r=\zeta^r.$$

若 $r\neq 0$，则与 d 是满足 $\zeta^d=1$ 的最小指数矛盾. 因而 $n=qd$，证毕. ■

→ **定义** 若 d 是一个正整数，则定义 d 次**分圆**[⊖]**多项式**为

$$\Phi_d(x)=\prod(x-\zeta),$$

其中 ζ 取遍所有 d 次本原单位根. 31

在命题 3.47 中，我们将证明 $\Phi_d(x)$ 的所有系数是整数.

下面这个结果几乎是显而易见的

命题 1.30 对每个整数 $n\geqslant 1$ 有

$$x^n-1=\prod_{d\mid n}\Phi_d(x),$$

其中 d 取遍 n 的所有正因子[特别地，$\Phi_1(x)$ 和 $\Phi_n(x)$ 都出现].

证明 根据推论 1.28，对 n 的每个因子 d，在方程 $x^n-1=\prod(x-\zeta)$ 中消去所有含 d 次本原单位根 ζ 的项即得证. ■

例如，若 p 是一个素数，则 $x^p-1=\Phi_1(x)\Phi_p(x)$. 因为 $\Phi_1(x)=x-1$，所以

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

→ **定义** **欧拉 ϕ-函数**是指 n 次分圆多项式的次数：

$$\phi(n)=\deg(\Phi_n(x)).$$

在命题 1.42 中，我们将给出欧拉 ϕ-函数不依赖于单位根的另一种描述.

推论 1.31 对每个整数 $n\geqslant 1$，我们有

$$n=\sum_{d\mid n}\phi(d).$$

证明 注意到 $\phi(n)$ 是 $\Phi_n(x)$ 的次数，并利用多项式的积的次数是其因子的次数的总和这个事实即得证. ■

三角函数的名称是从哪里来的呢？图 1-9 中的圆是单位圆，因此点 A 的坐标是$(\cos\alpha, \sin\alpha)$，即 $|OD|=\cos\alpha$，$|AD|=\sin\alpha$. 读者可以证明 $|BC|=\tan\alpha$（拉丁词 tangere 意思是“接触”，而“切线”(tangent)是指与单位圆仅在一点处接触的直线），且 $|OB|=\sec\alpha$（拉丁词 secare 意思是“切割”，而“割线”(secant)是指与圆切割的直线）. 一个锐角 α 的余角是 $90°-\alpha$，因为有恒等式 $\cos\alpha=\sin(90°-\alpha)$，因此余弦产生于正弦.

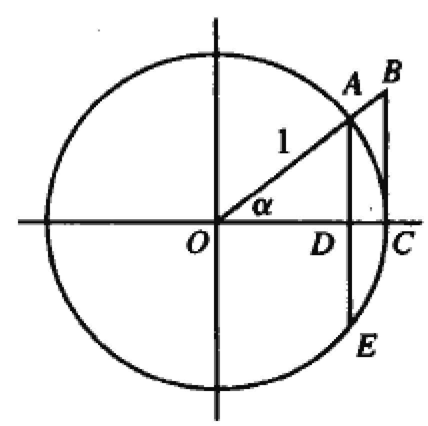


图 1-9 三角名称的由来

我在牛津英语字典中发现正弦的名称来由更有趣. 观察图 1-9 知

$$\sin\alpha=|AD|=\frac{1}{2}|AE|,$$ 32

即 $\sin\alpha$ 是弦 AE 长度的一半. 5 世纪印度数学家阿耶波多(Aryabhata)在梵语中称正弦为 ardha-jya（半弦），后来缩写为 jya. 几个世纪之后，用阿拉伯语写的书把 jya 变成 jiba. 在阿拉伯手稿中，有这样一些字母和变音符号，粗略地说，这些字母对应于我们的辅音字母，而变音

⊖ x^n-1 的根是 n 次单位根：$1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$，其中 $\zeta=e^{2\pi i/n}=\cos(2\pi/n)+i\sin(2\pi/n)$. 这些根把单位圆 $\{\zeta\in\mathbb{C}: |z|=1\}$ 分成 n 个相等的弧（见图 1-8）. 这解释了术语“分圆”(cyclotomic)，因为它的希腊语原意是“圆分裂”.

符号对应于我们的元音字母. 在写作中抑制这些变音符号是合乎习俗的, 例如, jiba 在阿拉伯语中写作 jb(当然用的是阿拉伯语特征). 现在, jiba 在阿拉伯语中已经没有其他意思了, 所以最终演变为 jaib, 这是一个阿拉伯词语, 意思是"一件衣服的胸部"(一个不错的词语, 但是绝对与半弦毫无关系). 最后, 大约 1150 年格拉多(Gherardo)把 jaib 翻译为拉丁文中的等价词语 sinus. 这就是为什么正弦是如此称呼的, 原因就在于正弦意思是胸部!

只要我们在讨论词源学, 就会问为什么这样称呼一个根呢? 正如希腊人称一个矩形的底边为底一样$\left(\text{例如面积公式为}\frac{1}{2}\text{高}\times\text{底}\right)$, 他们也称一个正方形的底边为底. 希腊人的一个问题是: 给定一个面积为 A 的正方形, 它的底的长度是多少? 回答当然是$\sqrt{A}$. 如果我们为$\sqrt{A}$取个名字, 那可能会称它为 A 的底或 A 的边. 类似地, 如果我们为下面的三维问题寻找一个术语: 一个体积为 V 的立方体的边长是多少? 我们可能会称$\sqrt[3]{V}$为 V 的立方底, 称$\sqrt{A}$为 A 的平方底. 那么, 为什么我们要称这些数字为立方根或平方根呢?

追踪这些词的来源不是一件简单的事情, 我们只给出下述解释. 大约在四世纪和五世纪之间, 许多数学家用希腊语写作, 但是, 到了五世纪末, 印度成为数学的中心, 许多重要的数学
33 文献也是用梵语写的. 平方根在梵语中称为 pada. 梵语和希腊语都是印欧语系, 梵语 pada 等同于希腊语 podos, 两者的意思都是指一根台柱的底部, 或者如上所述, 是指一个正方形的底部. 然而, 在这两种语言中, 该词还有另一种含义: 植物的根. 从梵语翻译过来时, 阿拉伯数学家选择了第二种含义, 也许这样做是错误的(阿拉伯语不是印欧语系), 也许是由于某个不为人所知的原因. 例如, 阿尔-瓦理斯米(al-Khwarizmi)写过一部很有影响的书《Al-jabr w'al muqabala》(《代数学》),[⊖]它是在 830 年出版的, 书中用的是阿拉伯词 jidhr, 意思是植物的根. (术语 algebra 是该书欧洲版书名中的第一个词, 其作者的名字也以词 algorithm 进入到了英语中.)这种错误翻译从那时开始流传下来, 经过了几个世纪, 术语 jidhr 成为阿拉伯数学写作中的标准术语, 欧洲人把阿拉伯语翻译成拉丁语时, 用的是词语 radix(意思是根). 大约从十二世纪开始, $\sqrt{2}$的记号 $r2$ 已经出现在欧洲的一些文章中(但是平方根的符号没有从字母 r 中演变出来, 它是由一个古老的圆点记号演变而来的). 然而, 同时存在一个有竞争的记号, 某些学者在直接翻译希腊语时, 记$\sqrt{2}$为 $l2$, 其中 l 是拉丁词 latus 的缩写, 意思是边. 最后, 随着 16 世纪对数的发明, r 战胜 l, 因为记号 $l2$ 在那时被普遍用来表示 log2. 本章从平方根到立方根再到除 x^2-a 和 x^3-a 以外的多项式方程的根的叙述是十分自然的. 因此, 似乎不存在方程的根与植物学之间的联系.

习题

H 1.28 判断对错并说明理由.

(i)对所有满足 $0<r<7$ 的整数 r, 二项式系数$\binom{7}{r}$是 7 的倍数.

⊖ 人们虽然可以翻译这个阿拉伯语标题, 但是这些词已经有了专门的含义: jabr 和 muqabala 都是指某种类似于从方程的两边减去一个相同的数的操作.

(ii)对任意整数 n 和任意满足 $0<r<n$ 的 r，二项式系数 $\binom{n}{r}$ 是 n 的倍数. 34

(iii)设 D 是 10 只不同的狗构成的集合，C 是 10 只不同的猫构成的集合，则狗的四重奏和猫的六重奏曲一样多.

(iv)若 q 是一个有理数，则 $e^{2\pi iq}$ 是一个单位根.

(v)设 $f(x)=ax^2+bx+c$，其中 a，b，c 都是实数. 若 z 是 $f(x)$ 的一个根，则 $\bar{z}$ 也是 $f(x)$ 的根.

(vi)设 $f(x)=ax^2+bx+c$，其中 a，b，c 都是复数. 若 z 是 $f(x)$ 的一个根，则 $\bar{z}$ 也是 $f(x)$ 的根.

(vii)4 次本原单位根是 i 和 $-$i.

H 1.29　证明二项式定理对复数成立：若 u，v 都是复数，则

$$(u+v)^n=\sum_{r=0}^{n}\binom{n}{r}u^{n-r}v^r.$$

*1.30　证明二项式系数是"对称的"：

$$\binom{n}{r}=\binom{n}{n-r}$$

对所有 r，$0\leqslant r\leqslant n$ 成立.

***H** 1.31　证明：对每个 n，二项式系数的总和是 2^n：

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}=2^n.$$

1.32　**H** (i)证明：对每个 $n\geqslant 1$，二项式系数的"交错总和"是 0：

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\cdots+(-1)^n\binom{n}{n}=0.$$

(ii)利用(i)证明，对给定的 n，r 为偶数时所有 $\binom{n}{r}$ 的总和等于 r 为奇数时所有 $\binom{n}{r}$ 的总和.

H 1.33　证明：若 $n\geqslant 2$，则

$$\sum_{r=1}^{n}(-1)^{r-1}r\binom{n}{r}=0.$$

*1.34　设 $1\leqslant r\leqslant n$，证明

$$\binom{n}{r}=\frac{n}{r}\binom{n-1}{r-1}.$$

1.35　设 ε_1，…，ε_n 是复数，对所有 j 有 $|\varepsilon_j|=1$，其中 $n\geqslant 2$.

H (i)证明

$$\left|\sum_{j=1}^{n}\varepsilon_j\right|\leqslant\sum_{j=1}^{n}|\varepsilon_j|=n.$$

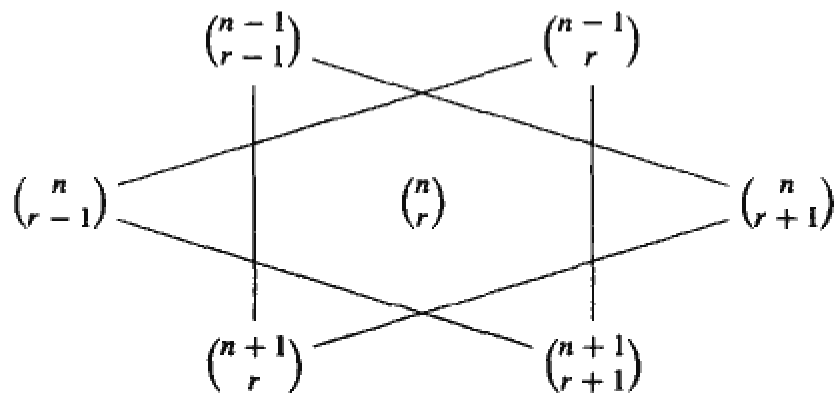
H (ii)证明

$$\left|\sum_{j=1}^{n}\varepsilon_j\right|=n$$

当且仅当所有 ε_j 都相等.

1.36　(**大卫的星**)证明：对所有 $n>r\geqslant 1$ 有

$$\binom{n-1}{r-1}\binom{n}{r+1}\binom{n+1}{r}=\binom{n-1}{r}\binom{n}{r-1}\binom{n+1}{r+1}.$$ 35



*H 1.37 对所有奇数 $n\geqslant 1$，证明存在一个整系数多项式 $g_n(x)$，使得

$$\sin(nx) = g_n(\sin x).$$

1.38 (i)$(1+x)^{20}$ 中 x^{16} 的系数是多少？

H (ii)从放有 20 种不同颜色涂料的调色板中选出 4 种颜色的方法有多少种？

1.39 至少给出两种不同的方法证明一个含有 n 个元素的集合 X 恰有 2^n 个子集.

H 1.40 一周一次的彩票要求在 1 与 45 之间选出 5 个数来. 在一周结束时，5 个数字被随机地抽出，如果你选的数字与抽出的数字完全相同，你将赢得头奖. 你赢的机会是多少？

定义 对函数 $f(x)$ 归纳地定义它的 n **阶导数** $f^{(n)}(x)$：令 $f^{(0)}(x)$ 为 $f(x)$，若 $n\geqslant 0$，则定义 $f^{(n+1)}(x)=(f^{(n)})'(x)$.

1.41 假设逐项求导对幂级数成立：若 $f(x)=c_0+c_1x+c_2x^2+\cdots+c_nx^n+\cdots$，则导数 $f'(x)$ 的幂级数是

$$f'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1} + \cdots.$$

(i)证明 $f(0)=c_0$.

(ii)证明：对所有 $n\geqslant 0$ 有

$$f^{(n)}(x) = n!c_n + (n+1)!c_{n+1}x + x^2g_n(x),$$

其中 $g_n(x)$ 是一个幂级数.

(iii)证明：对所有 $n\geqslant 0$ 有 $c_n=f^{(n)}(x)(0)/n!$.（当然，这是泰勒公式.）

*H 1.42 （**莱布尼茨公式**）函数 f：$\mathbb{R}\to\mathbb{R}$ 称为 $\mathbf{C}^\infty$**-函数**，若它对每个 $n\geqslant 0$ 有 n 阶导数 $f^{(n)}(x)$. 证明，若 f 和 g 都是 C^∞-函数，则 $(fg)^{(n)}(x)=\sum_{k=0}^{n}\binom{n}{k}f^{(k)}(x)\cdot g^{(n-k)}(x)$.

36 1.43 求 $\sqrt{\mathrm{i}}$.

*1.44 (i)若 $z=r[\cos\theta+\mathrm{i}\sin\theta]$，证明

$$w = \sqrt[n]{r}[\cos(\theta/n) + \mathrm{i}\sin(\theta/n)]$$

是 z 的一个 n 次根，其中 $r\geqslant 0$.

(ii)证明 z 的每个 n 次根都具有形式 $\zeta^k w$，其中 ζ 是 n 次本原单位根，$k=0, 1, 2, \cdots, n-1$.

1.45 H (i)求 $\sqrt{8+15\mathrm{i}}$.

H (ii)求 $8+15\mathrm{i}$ 的所有四次根.

→1.3 最大公因子

除 Z（表示整数集）和 N（表示自然数集）之外，我们有必要再介绍一些常见数集的符号.

Q ＝所有有理数（或分数）的集合，即所有形如 a/b 的数，其中 a 和 b 都是整数且 $b\neq 0$（源于单词 quotient）

$\mathbb{R}$ =所有实数的集合

$\mathbb{C}$ =所有复数的集合

长除法是指：用非 0 整数 a 除整数 b 得到

$$\frac{b}{a}=q+\frac{r}{a},$$

其中 q 是整数且 $0\leqslant r/a<1$. 现在我们清除分母以得到完全在 $\mathbb{Z}$ 内的一种叙述.

→ **定理 1.32（除法算式）** *给定整数 a，b 且 $a\neq 0$，则存在唯一的整数 q，r 满足*

$$b=qa+r,0\leqslant r<|a|.$$

证明 我们将证明 $a>0$ 且 $b\geqslant 0$ 的特殊情形. 习题 1.47 要求读者给出定理的完整证明. 长除法是指求出满足 $qa\leqslant b$ 的最大整数 q，或者说，求形如 $b-qa$ 的最小非负整数. 我们将这一意义形式化.

设集合 C 是由所有形如 $b-na$ 的非负整数构成的集合，其中 $n\geqslant 0$. 因为 $b=b-0a\in C$（我们假设 $b\geqslant 0$）所以 $C\neq\varnothing$. 由最小数原理知 C 含有最小元，不妨设为 $r=b-qa(q\geqslant 0)$. 当然，由定义知 $r\geqslant 0$. 假设 $r\geqslant a$，则

$$b-(q+1)a=b-qa-a=r-a\geqslant 0.$$ 37

因而 $r-a=b-(q+1)a\in C$ 且 $r-a<r$，这与 r 是 C 中的最小整数矛盾，因此 $0\leqslant r<a$.

以下证明 q 和 r 的唯一性. 假设 $b=qa+r=q'a+r'$，其中 $0\leqslant r$，$r'<a$，则

$$(q-q')a=r'-r.$$

不妨假设 $r'\geqslant r$，则 $r'-r\geqslant 0$，因而 $q-q'\geqslant 0$. 假设 $q\neq q'$，则 $q-q'\geqslant 1$（因 $q-q'$ 是整数）. 因为 $a>0$，所以

$$(q-q')a\geqslant a.$$

另一方面，由于 $r'<a$，由命题 A.2 知

$$r'-r<a-r\leqslant a.$$

因此 $(q-q')a\geqslant a$ 而 $r'-r<a$，这与 $(q-q')a=r'-r$ 矛盾. 所以 $q=q'$ 并且 $r=r'$. ■

→ **定义** *设 a，b 是整数且 $a\neq 0$，除法算式中的整数 q 和 r 分别称为 a 除 b 的***商***和***余数***.*

例如，一个数 m 被 2 除后余数有两种可能，即 0 和 1. 若余数是 0，则 m 是偶数；若余数是 1，则 m 是奇数. 因此 $m=2q$ 或 $m=2q+1$.

注意：当 b 是负整数时，除法算式也是有其意义的. 粗心的人可能认为 a 除 b 和 a 除 $-b$ 所得余数相同，但这通常是错误的. 例如，用 7 除 60 和 7 除 -60：

$$60=7\cdot 8+4,\quad -60=7\cdot(-9)+3.$$

可见 7 除 60 和 7 除 -60 所得余数是不同的（见习题 1.84）.

下述结果表明不存在最大的素数.

→ **推论 1.33** *素数有无穷多个.*

证明（欧几里得证法） 假设只有有限多个素数，用 p_1，p_2，…，p_k 表示所有的素数. 定义 $M=(p_1\cdots p_k)+1$. 由定理 1.2 知 M 或是素数，或是素数的积. 但是 M 既不是素数（$M>p_i$，$i=1$，…，k）也没有任何素数因子 p_i，这是因为 p_i 除 M 得余数 1 而不是 0. 例如，用 p_1 除 M 得

$M=p_1(p_2\cdots p_k)+1$，所以商和余数分别为 $q=p_2\cdots p_k$ 和 $r=1$；用 p_2 除 M 得 $M=p_2(p_1p_3\cdots p_k)+1$，
38 所以 $q=p_1p_3\cdots p_k$ 和 $r=1$，等等．这与素数只有有限多个相矛盾，因此素数有无穷多个． ■

算法是指一些命令的集合，这些命令经过有限步后给出正确答案，使问题得以解决．在这种意义上，除法算式是一种算法：我们从 a，b 开始，到 q，r 结束．书的末尾附录 B 中用**伪码**来更加正式地表示算法．伪码是一般的命令，它容易被翻译成程序设计语言．例如，下面是除法算式的一个伪码．

```
Input : b ≥ a > 0
Output : q,r
q := 0; r := b
WHILE r ≥ a DO
r := r − a
q := q + 1
END WHILE
```

→ **定义** *设 a，b 是整数，若存在整数 d 使得 $b=ad$，则称 a 是 b 的一个***因子***（也称 a* **整除** *b 或称 b 是 a 的***倍数***），记为*

$$a \mid b.$$

注意：$3\mid 6$，这是因为 $6=3\times 2$，但 $3\nmid 5$（即，3 不能整除 5），这是因为即使 $5=3\times\frac{5}{3}$，但 $\frac{5}{3}$ 不是整数．± 1 和 $\pm b$ 是任意整数 b 的因子．$b\mid 0$ 恒成立（因 $0=b\times 0$）；另一方面，若 $0\mid b$ 则 $b=0$（因为存在 d 使 $b=0\times d=0$）．

设 a，b 是整数且 $a\neq 0$，则 a 是 b 的因子当且仅当除法算式中余数 $r=0$．若 a 是 b 的一个因子，则除法算式中余数 $r=0$；反之，若余数 $r=0$，则 a 是 b 的一个因子．

→ **定义** *若整数 c 满足 $c\mid a$，$c\mid b$，则 c 称为整数 a 和 b 的***公因子***．a 和 b 的***最大公因子***记为 $\gcd(a, b)$［或简记为 (a, b)］，其定义为*

$$\gcd(a,b)=\begin{cases}0, & \text{当 } a=0=b\\ a,b\text{ 最大的公因子}, & \text{其他}\end{cases}$$

显然，最大公因子的记号 (a, b) 同有序对使用的记号是一样的，但是读者根据这个符号所在的上下文应当不难理解符号的含义．

设 a 和 m 是正整数且 $a\mid m$，不妨设 $m=ab$，我们断言 $a\leqslant m$．由于 $0<b$，又因为 b 是整
39 数，所以 $1\leqslant b$，这样 $a\leqslant ab=m$．于是最大公因子总是存在的．

若 c 是 a 和 b 的一个公因子，则 $-c$ 也是．因为 $\pm c$ 当中有一个是非负的，所以最大公因子总是非负的．若 a 和 b 至少有一个非零，则 $(a, b)>0$．

命题 1.34 *设 p 是素数，b 是任意整数，则*

$$\gcd(p,b)=\begin{cases}p & \text{当 } p\mid b\\ 1 & \text{其他.}\end{cases}$$

证明 p 和 b 的公因子 c 当然是 p 的一个因子，但 p 的正因子只有 p 和 1，所以 $(p, b)=$

p 或 1. 若 $p \mid b$，则 $(p, b)=p$，否则 $(p, b)=1$. ■

→ **定义** 整数 a，b 的一个线性组合是指形如

$$sa + tb$$

的整数，其中 s，t 为整数.

下述结果是最大公因子的一个最有用的性质.

→ **定理 1.35** 若 a，b 是整数，则 $\gcd(a, b)$ 是 a，b 的一个线性组合.

证明 我们可假设 a 和 b 至少有一个不为 0(否则最大公因子是 0，结论显然成立). 考虑由 a 和 b 的所有线性组合构成的集合 I：

$$I = \{sa + tb : s,t \in \mathbb{Z}\}.$$

现在 $a\in I$(取 $s=1$，$t=0$)，$b\in I$(取 $s=0$，$t=1$). 于是 I 含有正整数(若 $a\neq 0$，则 I 含有 $\pm a$)，因而由 I 中所有正整数构成的集合 $P\neq\varnothing$. 由最小数原理知 P 含有最小正整数，不妨设为 d，我们断言 d 是 a 和 b 的最大公因子.

由于 $d\in I$，所以 d 是 a，b 的一个线性组合：存在整数 s，t，使

$$d = sa + tb.$$

让我们通过证明 d 既整除 a 也整除 b 来证明 d 是 a 和 b 的公因子. 由除法算式知 $a=qd+r$，其中 $0\leqslant r<d$. 若 $r>0$，则

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b \in P,$$

此与 d 是 P 的最小元矛盾. 因而 $r=0$，我们有 $d \mid a$. 类似的讨论可证得 $d \mid b$.

若 c 是 a 和 b 的一个公因子，则 $a=ca'$，$b=cb'$，因为 $d=sa+tb=c(sa'+tb')$，所以 $c \mid d$. 又若 $c \mid d$，则 $|c| \leqslant d$，所以 d 是 a 和 b 的最大公因子. ■

若 $d=\gcd(a, b)$，c 是 a 和 b 的一个公因子，则 $c\leqslant d$. 下面的推论表明：对每个公因子 c 都有 $c \mid d$. 40

→ **推论 1.36** 设 a，b 是整数，非负公因子 d 是它们的最大公因子当且仅当对每个公因子 c 都有 $c \mid d$.

证明 必要性($\Rightarrow$)：定理 1.35 的证明结尾部分已经证明了 a 和 b 的每个公因子 c 是 $d=sa+tb$的一个因子.

充分性($\Leftarrow$)：设 d 是 a 和 b 的最大公因子，d'是可被每个公因子 c 整除的非负公因子. 因此 $d'\leqslant d$，这是因为对每个公因子 c 有 $c\leqslant d$. 另一方面 d 本身是一个公因子，所以根据假设有 $d \mid d'$，因而 $d\leqslant d'$，所以 $d=d'$. ■

定理 1.35 的证明还包含了一个将要再次用到的思想.

→ **推论 1.37** 设 I 是$\mathbb{Z}$ 的一个子集，满足

(i) $0\in I$；

(ii) 若 a，$b\in I$，则 $a-b\in I$；

(iii) 若 $a\in I$，$q\in \mathbb{Z}$，则 $qa\in I$.

则存在非负整数 $d\in I$，使得 I 恰由 d 的所有倍数构成.

证明 若 $I=\{0\}$，则取 $d=0$. 若 I 含有非零整数 a，则由(iii)知 $(-1)a=-a\in I$，因此

$\pm a\in I$，其中之一为正数．由最小数原理，I 含有最小正整数，记为 d.

我们断言，每个 $a\in I$ 是 d 的一个倍数．由除法算式知，存在整数 q，r 使 $a=qd+r$，$0\leqslant r<d$．由于 $d\in I$，所以由(iii)知 $qd\in I$，又由(ii)知 $r=a-qd\in I$．但 $r<d$，而 d 是 I 的最小正整数，所以 $r=0$．因此 a 是 d 的一个倍数． ■

下述结果被称为欧几里得引理，它是非常有趣的，因为它给出了素数的一个非常重要的特征．欧几里得引理经常被使用(仅在本章中就至少使用了 10 次)，对于不可约多项式它的类似结论也是非常重要的．进一步看，这个引理还引出了素理想的概念．

→ **定理 1.38(欧几里得引理)** *若 p 是素数且 $p\mid ab$，则 $p\mid a$ 或 $p\mid b$．更一般地，若素数 p 整除 $a_1a_2\cdots a_n$，则 p 至少整除其中一个因子 a_i．反之，若整数 $m\geqslant 2$ 满足：当 $m\mid ab$ 时总有 $m\mid a$ 或 $m\mid b$，则 m 是一个素数.*

证明 假设 $p\nmid a$，我们必须证明 $p\mid b$．由命题 1.34 知 $(p, a)=1$，又由定理 1.35 知存在整数 s，t 使得 $1=sp+ta$，所以

41
$$b = spb + tab.$$

因为 $p\mid ab$，所以存在整数 c 使得 $ab=pc$，因此 $b=spb+tpc=p(sb+tc)$，$p\mid b$．第二个命题对 $n\geqslant 2$ 用归纳法容易得到．

证明逆命题：假设 m 是合数，则 $m=ab$，其中 $a<m$，$b<m$．这样 $m\mid ab$，由题设知 $m\mid a$ 或 $m\mid b$，但 m 不能整除 a，b(因为 $a<m$，$b<m$)，矛盾． ■

这里有一个具体实例可以说明欧几里得引理在一般情况下不成立：$6\mid 12=4\times 3$，但 $6\nmid 4$，$6\nmid 3$.

→ **命题 1.39** *若 p 是素数，则 $p\mid \binom{p}{j}$，$0<j<p$.*

证明 回忆

$$\binom{p}{j}=\frac{p!}{j!(p-j)!}=\frac{p(p-1)\cdots(p-j+1)}{j!}.$$

交叉相乘后得

$$j!\binom{p}{j}=p(p-1)\cdots(p-j+1),$$

所以 $p\mid j!\binom{p}{j}$．若 $p\mid j!$，则由欧几里得引理知 p 一定能整除 $j!$ 的某个因子 $1, 2, \cdots, j$．但由于 $0<j<p$，所以 $j!$ 的每个因子都严格小于 p，因此 p 不是它们任何一个的因子，因此 $p\nmid j!$．因为 $p\mid j!\binom{p}{j}$，所以由欧几里得引理知 $p\,\Big|\binom{p}{j}$． ■

注意：命题中假设 p 是素数是必要的，例如 $\binom{4}{2}=6$，但 $4\nmid 6$.

→ **定义** *若整数 a 和 b 的最大公因子是 1，则称 a 和 b* **互素**.

这样，若 a 和 b 的公因子只有 ± 1，则它们互素且 1 是 a 和 b 的线性组合．例如，2 和 3 互

素，8 和 15 互素.

以下是欧几里得引理的一个推论，其证明相同.

→ **推论 1.40** *设 a，b，c 是整数. 若 c 和 a 互素且 $c \mid ab$，则 $c \mid b$.*

证明 由条件知存在某个整数 d 使得 $ab=cd$. 又因为存在整数 s，t 使得 $1=sc+ta$，所以 $b=scb+tab=scb+tcd=c(sb+td)$. ■

弄清楚这两个结论的证明是很重要的：推论 1.40 虽然不是欧几里得引理的延续，但其证明却是. 42

定义 *若 a 和 b 互素，则称有理数 a/b(其中 a，b 是整数)的表示式是**既约的**.*

引理 1.41 *每个非零有理数 r 都有既约表示式.*

证明 由于 r 是有理数，所以存在整数 a，b 使得 $r=a/b$. 若 $d=(a, b)$，则 $a=a'd$，$b=b'd$，$a/b=a'd/b'd=a'/b'$. 但 $(a', b')=1$，这是因为若 $d'>1$ 是 a'，b' 的一个公因子，则 $d'd>d$ 是 a，b 的一个更大的公因子. 矛盾！ ■

以下是对没有提到分圆多项式的欧拉 ϕ-函数的一个描述. 回忆 $\phi(n)$ 被定义为 n 次本原单位根 ζ 的个数，即 $\zeta^n=1$，但是对 $1\leqslant d<n$ 有 $\zeta^d\neq 1$.

→ **命题 1.42** *若整数 $n\geqslant 1$，则 $\phi(n)$ 是满足 $1\leqslant k\leqslant n$ 和 $(k, n)=1$ 的整数 k 的个数.*

证明 根据推论 1.28，因为每个 n 次单位根有形式 $\zeta=e^{2\pi ik/n}$，所以只需证明 ζ 是本原的当且仅当 $(k, n)=1$.

若 k 和 n 不互素，则 $n=dr$，$k=ds$，其中 d，r，s 都是整数，且 $d>1$，所以 $r<n$. 因而 $\frac{k}{n}=\frac{ds}{dr}=\frac{s}{r}$，因而 $(e^{2\pi ik/n})^r=(e^{2\pi is/r})^r=1$，$e^{2\pi ik/n}$ 不是一个 n 次本原单位根，矛盾.

反之，假设 $(k, n)=1$. 记 $\zeta=e^{2\pi ik/n}$，$\eta=e^{2\pi i/n}$. 存在整数 s，t 使 $sk+tn=1$. 因而

$$\eta = e^{2\pi i/n} = e^{2\pi iks/n}e^{2\pi itn/n} = e^{2\pi iks/n} = \zeta^s.$$

若存在 d 满足 $1\leqslant d<n$，则 $\zeta^d=1$，$\eta^d=1$，这与 η 是一个 n 次本原单位根矛盾. 因此，这样的 d 不存在，ζ 是一个 n 次本原单位根. ■

命题 1.43 *$\sqrt{2}$ 是无理数.*

证明 假设 $\sqrt{2}$ 是有理数，即 $\sqrt{2}=a/b$. 我们可假设 a/b 是既约的，即 $(a, b)=1$. 两边平方得 $a^2=2b^2$. 由欧几里得引理[⊖]知 $2 \mid a$，所以 $2m=a$，因而 $4m^2=a^2=2b^2$，$2m^2=b^2$. 此时又由欧几里得引理知 $2 \mid b$，这与 $(a, b)=1$ 矛盾. ■

命题 1.43 在数学史上是有特殊意义的. 古希腊人定义的数是指“正整数”，而(正)有理数被看作是“比率” $a:b$ (我们可以把它解释为分数 a/b). $\sqrt{2}$ 是无理数，这对毕达哥拉斯学派(约公元前 600 年)来说是震惊的，因为这告诉他们 $\sqrt{2}$ 不能仅用数(正整数)的观点来定义. 另一方面，他们认识到边长为 1 的正方形的对角线的长度是 $\sqrt{2}$. 因此，方程 $x^2=2$ 没有数解但有几何解. 到了欧几里得那个时代(约公元前 325 年)，通过把数学分成两个学科：代数学和几何学，这个问题才被解决. 这个问题的解决可能是经典数学的黄金时期起源于罗马帝国而后在欧洲衰 43

⊖ 这个证明可以更初等些，只需利用命题 1.14.

退的主要原因之一．例如，看待线段的加、减、乘、除(见定理 4.47)有一些几何方法，但实际上不可能做任何代数运算．需要一个复杂的几何论断[归功于欧多克索斯(Eudoxus)，见欧几里得的《几何原本》]才能证明交叉相乘成立，即若 $a:b=c:d$，则 $a:c=b:d$.

我们引用《科学启发》(*Science Awakening*)第 125 页范·德·瓦尔登(van der Waerden)说的话：

如今我们说对角线的长度$\sqrt{2}$是"无理数"，并感觉比贫穷的"不知道无理数"的希腊人更优越，但是希腊人非常了解无理数率……他们不认为$\sqrt{2}$是一个数，这不是疏忽的结果，而是对数的定义的严格坚持．希腊文字"arithmos(数字)"的意思是数量，因此是指完整的数．他们逻辑上的严格甚至不允许他们承认分数，所以他们用整数的比来代替．

对巴比伦人来说，每条线段，每块面积只表示一个数……当他们不能确定平方根的确切值时，就镇静地接受一个近似值．工程师和自然科学家们已经是这样做了．但是希腊人关心精确的知识，要的是"对角线本身"，如柏拉图所表达的，而不是一个可接受的近似值．

在数(正整数)的范围内，方程 $x^2=2$ 不能解，甚至不能用数的比表示出来，但在线段的范围内方程有解．事实上，单位正方形的对角线是一个解．因此，为了得到二次方程的精确解，我们不得不由数(正整数)的范围过渡到几何的范围．几何代数对无理线段也是有效的，并依然是一门精确的科学．因此，是逻辑上的需要，而不是视觉上的愉快，迫使毕达哥拉斯将他们的代数学改变为一种几何形式．

即使数的希腊定义不再流行，但是它们的划分依然存留了下来．例如，几乎所有的美国高中都是教一年代数后再教一年几何，而不是两年中两门课程一起教．从古希腊时代以来，出现过几次定义数的问题．在 16 世纪，数学家们不得不处理负数和复数(见第 5 章中对三次多项式的讨论)．今天普遍接受的实数的描述，是自 19 世纪后期延用至今的．在我们这个时代，存在
44 一些古雅典娜的附和者．例如，克罗内克(L. Kronecker，1823—1891)写道：

上帝创造了数，其他一切都是人为的．

甚至今天还有一些逻辑学家坚持要给数一个新的定义．

我们对最大公因子的讨论还未结束．gcd(12327，2409)是多少？用另一种方式问这个问题，表达式 2409/12327 是既约的吗？下面这个结果不仅使我们可以高效率地计算最大公因子，而且还可以计算把最大公因子表示成一个线性组合时所需的整数 s 和 t．[⊖]在给出这个定理之前，思考下述例子．因为$(2,3)=1$，所以存在整数 s 和 t 使得 $1=2s+3t$．考虑一会儿就知道 $s=-1$，$t=1$，但又一想，得 $s=2$，$t=-1$．我们得出结论，把最大公因子表示成线性组合的系数 s 和 t 不是唯一的．然而，下面的算法总可以选出一对特殊的系数来．

→ **定理 1.44(欧几里得算法)** *设 a，b 是正整数，则存在求最大公因子 $d=(a,b)$ 的一种算法，且存在求一对整数 s，t 使得 $d=sa+tb$ 的算法．*

注 因为$(a,b)=(|a|,|b|)$，所以关于任意 a，b 的一般情形也可以解决．

⊖ 每个正整数都是一些素数的积，命题 1.55 将使用该结论去计算最大公因子．然而，寻找大数的素分解是困难的，实际上，这正是公众密码系统安全的基本原因．

证明 证明的思想是反复应用除法算式(我们将会在证明完成之后看到这种思想是从何而来的). 令 $b=r_0$, $a=r_1$, 反复应用除法算式, 得如下整数 q_i, 正整数 r_i 和方程:

$$\begin{aligned} b &= q_1 a + r_2, & r_2 &< a \\ a = r_1 &= q_2 r_2 + r_3, & r_3 &< r_2 \\ r_2 &= q_3 r_3 + r_4, & r_4 &< r_3 \\ &\vdots & &\vdots \\ r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1}, & r_{n-1} &< r_{n-2} \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, & r_n &< r_{n-1} \\ r_{n-1} &= q_n r_n \end{aligned}$$ 45

(记住, 由除法算式可知所有的 q_j 和 r_j 都是已知的). 首先注意到存在最后一个余数, 这是因为余数构成一个严格递减的非负整数序列, 所以过程会终止(事实上, 所需步骤少于 a 步. 命题 1.46 给出了步骤数目的更小上界).

我们利用推论 1.36 证明最后的余数是最大公因子. 重写欧几里得算法的最先两个等式为

$$\begin{aligned} b &= qa + r \\ a &= q'r + s. \end{aligned}$$

若 c 是 a, b 的公因子, 则第一个等式表明 $c \mid r$. 继续看第二个等式, 我们可知 $c \mid a$, $c \mid r$, 所以 $c \mid s$. 一直继续直到看最后一个等式, 我们看到 c 整除每个余数, 特别地, $c \mid d$.

现在重写欧几里得算法的最后几个等式为

$$\begin{aligned} f &= ug + h \\ g &= u'h + k \\ h &= u''k + d \\ k &= vd \end{aligned}$$

看最后一个等式, 知 $d \mid k$, $d \mid d$, 所以 $d \mid h$. 再往上看, 知 $d \mid h$, $d \mid k$, 所以 $d \mid g$. 最终得 $d \mid a$ 和 $d \mid b$. 由此知 d 是一个公因子. 但是, 因为我们在前面部分已经看到, 若 c 是任意一个公因子, 则 $c \mid d$, 所以 $d=(a, b)$.

我们现在求 s, t, 仍从底端往上算. 重写 $h=u'k+d$ 为 $d=h-u'k$, 并代入它上面的等式 $k=g-u'h$ 得

$$d = h - u''k = h - u''(g - u'h) = (1 + u''u')h - u''g.$$

因此, d 是 g 和 h 的一个线性组合. 继续这个步骤, 用 h 替代 $f-ug$, 等等, 直到 d 写成了 a 和 b 的一个线性组合. ∎

因为我们直到除法算式应用于 r_{n-1} 和 r_n 才知道第$(n-1)$步

$$r_{n-2} = q_{n-1} r_{n-1} + r_n$$

中的 r_n 是否是最大公因子, 所以我们称 n 为欧几里得算法中的步数.

例 1.45 求(326, 78), 将它表示成 326 和 78 的一个线性组合, 并写出 78/326 的既约形式. 46

$$\boxed{326} = 4 \times \boxed{78} + \boxed{14} \qquad (1)$$

$$\boxed{78} = 5 \times \boxed{14} + \boxed{8} \qquad (2)$$

$$\boxed{14}=1\times\boxed{8}+\boxed{6} \qquad (3)$$

$$\boxed{8}=1\times\boxed{6}+\boxed{2} \qquad (4)$$

$$\boxed{6}=3\times\boxed{2} \qquad (5)$$

由欧几里得算法知(326，78)=2.

现在利用上述过程将 2 表示成 326 和 78 的一个线性组合.

$$\begin{aligned}2&=\boxed{8}-1\,\boxed{6} && \text{利用}(4)\\&=\boxed{8}-1(\boxed{14}-1\,\boxed{8}) && \text{利用}(3)\\&=2\,\boxed{8}-1\,\boxed{14}=2(\boxed{78}-5\,\boxed{14})-1\,\boxed{14} && \text{利用}(2)\\&=2\,\boxed{78}-11\,\boxed{14}=2\,\boxed{78}-11(\boxed{326}-4\,\boxed{78}) && \text{利用}(1)\\&=46\,\boxed{78}-11\,\boxed{326};\end{aligned}$$

因此 $s=46$，$t=-11$.

用最大公因子 2 除分子和分母得 78/326=39/163，这就是要求的既约式. ◀

希腊人称欧几里得算法为 antanairesis 或 anthyphairesis，两个都可以翻译成“辗转相除法”. 习题 1.61 是说$(b,a)=(b-a,a)$. 若 $b-a\geqslant a$，则$(b,a)=(b-a,a)=(b-2a,a)$. 继续减下去，直到得一对 a 和 $b-qa$ 满足 $b-qa<a$. 因此，若 $r=b-qa$，其中 $0\leqslant r<a$，则

$$(b,a)=(b-a,a)=(b-2a,a)=\cdots=(b-qa,a)=(r,a).$$

现在改变方向：从$(r,a)=(a,r)$开始重复上述过程，其中 $a>r$，最终得$(d,0)=d$.

例如，用 antanairesis 算法计算最大公因子(326，78)如下：

47 $$(326,78)=(248,78)=(170,78)=(92,78)=(14,78).$$

到目前为止，我们都是用大的数减去 78. 此时，因为 78>14，所以减去 14(这正是 antanairesis 算法与欧几里得算法相反的方面)，

$$(78,14)=(64,14)=(50,14)=(36,14)=(22,14)=(8,14).$$

我们又互反一下得：

$$(14,8)=(6,8).$$

再互反一次得(8，6)=(2，6)，最后一次互反得

$$(6,2)=(4,2)=(2,2)=(0,2)=2.$$

因此，最大公因子(326，78)=2.

使用除法算式(刚刚被迭代相减!)对实施 antanairesis 算法会更有效. 从(326，78)到(14，78)有 4 步，用除法算式表示出来就是

$$326=4\times78+14.$$

从(78，14)到(8，14)有 5 步，用除法算式表示出来是

$$78=5\times14+8.$$

从(14，8)到(6，8)有 1 步，即

$$14=1\times8+6.$$

从(8，6)到(2，6)有1步，即

$$8 = 1 \times 6 + 2.$$

从(6，2)到(0，2)=2有3步，即

$$6 = 3 \times 2.$$

这些就是欧几里得算法中的步骤.

欧几里得算法是最早给出计算步骤数目的确切范围的算法之一. 下面这个结果的证明要考虑斐波那契序列

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad n \geqslant 2.$$ [48]

命题 1.46 (拉梅[⊖]定理) *设 $b \geqslant a$ 都是正整数，$d(a)$是 a 的十进制表示式中数字的个数. 若 n 是用欧几里得算法计算最大公因子(a, b)的步数，则*

$$n \leqslant 5d(a).$$

证明 在欧几里得算法的等式中，我们用 r_0 表示 b，r_1 表示 a，使得每个等式有形式

$$r_j = r_{j+1} q_{j+1} + r_{j+2}$$

除了最后一个，即

$$r_{n-1} = r_n q_n.$$

注意 $q_n \geqslant 2$：若 $q_n \leqslant 1$，则 $r_{n-1} \leqslant q_n r_n = r_n$，这与 $r_n < r_{n-1}$ 矛盾. 类似地，所有 q_1，q_2，…，$q_{n-1} \geqslant 1$：否则存在 $j \leqslant n-1$ 使得 $q_j = 0$ 且 $r_{j-1} = r_{j+1}$，与严格不等式 $r_n < r_{n-1} < \cdots < r_1 = b$ 矛盾.

现在

$$r_n \geqslant 1 = F_2$$

且由于 $q_n \geqslant 2$，

$$r_{n-1} = r_n q_n \geqslant 2r_n \geqslant 2F_2 \geqslant 2 = F_3.$$

更一般地，让我们对 $j \geqslant 0$ 应用归纳法证明

$$r_{n-j} \geqslant F_{j+2}.$$

归纳步骤为

$$\begin{aligned} r_{n-j-1} &= r_{n-j} q_{n-j} + r_{n-j+1} \\ &\geqslant r_{n-j} + r_{n-j+1} \quad (\text{因为 } q_{n-j} \geqslant 1) \\ &\geqslant F_{j+2} + F_{j+1} = F_{j+3}. \end{aligned}$$

所以 $a = r_1 = r_{n-(n-1)} \geqslant F_{n-1+2} = F_{n+1}$. 由推论 1.16 知 $F_{n+1} > \gamma^{n-1}$，其中 $\gamma = \frac{1}{2}(1+\sqrt{5})$，所以

$$a > \gamma^{n-1}.$$

因为 $\log_{10}\gamma > \log_{10}(1.6) > \frac{1}{5}$，所以

⊖ 这是定理不以其发现者的名字来命名的一个例子. 拉梅(Lamé)的证明出现在1844年. 对欧几里得算法中的步数 n 的最早估计可在1564年左右由西蒙·雅可布(Simon Jacob)编著的一本珍贵的书中找到. 还有一些其他的估计，分别由德. 拉格尼(T. F. de Lagny)在1733年，瑞奥德(A.-A.-L. Reynaud)在1821年，勒格(E. Léger)在1837年和芬克(P.-J.-E. Finck)在1841年得到. [这些更早的估计在刊物《Historia Mathematica》(《数学史》)中有描述，分别见于夏利特(P. Shallit，1994)和施雷伯(P. Schreiber，1995)的文章中.]

49 $$\log_{10} a > (n-1)\log_{10}\gamma > (n-1)/5.$$

因此

$$n-1 < 5\log_{10} a < 5d(a),$$

这里 $d(a)=\lfloor \log_{10} a \rfloor+1$，因为 $d(a)$是整数，所以 $5d(a)$是整数，所以 $n\leqslant 5d(a)$. ■

例如，因为 $d(78)=2$，所以拉梅定理保证了计算(326，78)至多需要 10 步；实际上只有 5 步.

整数 5754 是

$$5\times 10^3+7\times 10^2+5\times 10+4$$

的缩写. 下述结果表明 10 并不是什么有魔力的数，任意整数 $b\geqslant 2$ 可以代替 10 来使用.

→ **命题 1.47** *若 $b\geqslant 2$ 是整数，则每个正整数 m 有以 b 为底数的表达式：存在整数 d_i，$0\leqslant d_i<b$，使得*

$$m=d_k b^k+d_{k-1}b^{k-1}+\cdots+d_0;$$

而且，若 $d_k\neq 0$，则表达式是唯一的.

注 *数 d_k，…，d_0 称为 m 的* **b-进位数**.

证明 我们用如下的迭代除法算式来定义整数 a_i 和 d_i.

$$\begin{aligned} m &= a_0 b+d_0, \quad 0\leqslant d_0<b \\ a_0 &= a_1 b+d_1, \quad 0\leqslant d_1<b \\ a_1 &= a_2 b+d_2, \quad 0\leqslant d_2<b \\ &\vdots \qquad\qquad\qquad \vdots \end{aligned}$$

简单的归纳表明 $m=b^{i+1}a_i+b^i d_i+b^{i-1}d_{i-1}+\cdots+bd_1+d_0$. 存在一个整数 k 满足 $b^k\leqslant m<b^{k+1}$. 对这个 k，我们有 $a_k=0$(若 $a_k\neq 0$，则 $a_k\geqslant 1$ 且 $m\geqslant b^{k+1}a_k\geqslant b^{k+1}$). 因而

$$m=b^k d_k+b^{k-1}d_{k-1}+b^{k-2}d_{k-2}+\cdots+bd_1+d_0$$

是 m 的以 b 为底数的表达式.

在证明数字 d_i 的唯一性之前，我们首先观察到，若对所有 i 有 $0\leqslant d_i<b$，则

50 $$\sum_{i=0}^{k} d_i b^i \leqslant \sum_{i=0}^{k}(b-1)b^i = \sum_{i=0}^{k} b^{i+1} - \sum_{i=0}^{k} b^i = b^{k+1}-1 < b^{k+1}. \tag{6}$$

现在对 $k\geqslant 0$ 应用归纳法证明：若 $b^k\leqslant m<b^{k+1}$，则表示式 $m=\sum_{i=0}^{k} d_i b^i$ 中 b-进位数 d_i 是由 m 唯一确定的. 设 $m=\sum_{i=0}^{k} d_i b^i=\sum_{i=0}^{k} c_i b^i$，其中对所有 i 有 $0\leqslant d_i<b$，$0\leqslant c_i<b$. 两式相减后得

$$0=\sum_{i=0}^{k}(d_i-c_i)b^i.$$

排除任意零系数，并将所有负系数 d_i-c_i(如果还有的话)颠倒顺序，从而得到一个等式：

$$L=\sum_{i\in I}(d_i-c_i)b^i=\sum_{j\in J}(c_j-d_j)b^j=R,$$

其所有系数为正数，且指标集 I 和 J 不相交. 设 p 是 I 中的最大指标，q 是 J 中的最大指标.

因为 I 和 J 不相交，所以我们可假设 $q<p$. 因为左边 L 含有 b^p，其系数不为零，所以 $L\geqslant b^p$；但由(6)知右边 $R<b^{q+1}\leqslant b^p$，矛盾. 因此 b-进位数 d_i 是唯一确定的. ■

例 1.48　让我们紧接命题 1.47 的证明过程，写出 12 345 的以 7 为底数的表示式. 反复利用除法算式得

$$\begin{aligned}12\,345 &= 1763\times 7+4\\ 1763 &= 251\times 7+6\\ 251 &= 35\times 7+6\\ 35 &= 5\times 7+0\\ 5 &= 0\times 7+5.\end{aligned}$$

因此 12 345 的 7-进位数是 50 664. ◀

最常用的底数是 $b=10$（给出了每个十进制数字），$b=2$（给出了二进制数字，这是很有用的，因为计算机可以把 1 解释为"on"，把 0 解释为"off"），以及 $b=16$（十六进制，也用于计算机），不过，其他的底数也是有用的，让我们来看一下.

例 1.49　以下是梅齐利亚克(Bachet de Méziriac)在 1624 年提出的一个问题. 一个商人有一个重 40 磅的东西碎成了 4 块，在称这些碎块时发现：每个碎块的重量都是整数，并且可以用这 4 块碎块来称重量介于 1 到 40 磅之间且为整数的物体. 那么这 4 块碎块的重量分别是多少呢？ 51

称重是指用一个有两个托盘的天平，把物体放在任何一个托盘中去称重量. 给定 1 磅和 3 磅的物体，人们可以称出 2 磅的物体□，其方法是：在一个托盘中放上 1 磅的物体和待称的物体□，而在另一个托盘放上 3 磅的物体.

梅齐利亚克问题的答案是 1，3，9，27. 用□表示给定的整数磅重的物体，我们记下两个托盘中物体的重量，并用分号相隔，黑体数字是□的重量，读者应当注意到，命题 1.47 给出了放在托盘中的重量的唯一性.

1	1;□	**9**	9;□
2	3;1,□	**10**	9,1;□
3	3;□	**11**	9,3;1,□
4	3,1;□	**12**	9,3;□
5	9;3,1,□	**13**	9,3,1;□
6	9;3,□	**14**	27;9,3,1,□
7	9,1;3,□	**15**	27;9,3,□
8	9;1,□		

读者可以对□≤40 完成这个表格. ◀

例 1.50　给定一个天平，则任何体重不超过 364 磅的人的体重(整数磅)可以只利用 6 个铅块来称出.

我们先证明每个正整数 m 可以写成

$$m=e_k3^k+e_{k-1}3^{k-1}+\cdots+3e_1+e_0,$$

其中 $e_i=-1$，0 或 1.

现在修改这个 3-进位数表达式为

$$m = d_k 3^k + d_{k-1} 3^{k-1} + \cdots + 3d_1 + d_0,$$

其中 $d_i=0, 1, 2$. 若 $d_0=0$ 或 1，则令 $e_0=d_0$，留下 d_1. 若 $d_0=2$，则令 $e_0=-1$，并用 d_1+1 代替 d_1(我们只要把 2 换成 $3-1$). 现在 $1\leqslant d_1+1\leqslant 3$. 若 $d_1+1=1$，则令 $e_1=1$，并留下 d_2. 若 $d_1+1=2$，则令 $e_1=-1$，并用 d_2+1 代替 d_2. 若 $d_1+1=3$，则定义 $e_1=0$，并用 d_2+1 代
52 替 d_2. 如此继续下去(m 的最后表达式可以从 $e_k 3^k$ 或 $e_{k+1}3^{k+1}$ 开始). 以下是这个新表达式中最先的几个数被列出的一个表(我们用 $\bar{1}$ 代替 -1).

1	1	**9**	1 0 0
2	1 $\bar{1}$	**10**	1 0 1
3	1 0	**11**	1 1 $\bar{1}$
4	1 1	**12**	1 1 0
5	1 $\bar{1}$ $\bar{1}$	**13**	1 1 1
6	1 $\bar{1}$ 0	**14**	1 $\bar{1}$ $\bar{1}$ $\bar{1}$
7	1 $\bar{1}$ 1	**15**	1 $\bar{1}$ $\bar{1}$ 0
8	1 0 $\bar{1}$		

读者现在应当理解了例 1.49. 若□重 m 磅，记 $m=\sum e_i 3^i$，其中 $e_i=1$，0 或 -1，则把系数为负的那些项颠倒一下. 这些使 $e_i=-1$ 的物体与□放在同一个托盘中，而其他使 $e_i=1$ 的物体放在另一个托盘中.

要解决当前的称重问题，需要选取重量分别为 1，3，9，27，81 和 243 磅的铅块. 我们可以称出体重在 365 磅以下的任何人的重量，这是因为 $1+3+9+27+81=364$. ◀

习题

H 1.46 判断对错并说明理由.

(i) $6 \mid 2$.

(ii) $2 \mid 6$.

(iii) $6 \mid 0$.

(iv) $0 \mid 6$.

(v) $0 \mid 0$.

(vi) 对每个自然数有 $(n, n+1)=1$.

(vii) 对每个自然数有 $(n, n+2)=2$.

(viii) 若 b，m 都是正整数，则 $b \mid m$ 当且仅当 m 的最后一个 b-进位数 d_0 是 0.

(ix) 113 是 2 的不同幂的和.

(x) 若 a，b 都是自然数，则存在自然数 s 和 t 使得 $\gcd(a, b)=sa+tb$.

***H 1.47** 给定整数 a 和 b(可能为负数)满足 $a\neq 0$，证明存在唯一的整数 q 和 r 使得 $b=qa+r$ 和 $0\leqslant r<|a|$.

1.48 不用欧几里得引理而用命题 1.14 证明 $\sqrt{2}$ 是无理数.

H 1.49 设 $p_1, p_2, p_3, \cdots$ 是按递增顺序排列的素数：$p_1=2$，$p_2=3$，$p_3=5$ 等等. 对 $k\geqslant 1$ 定义 $f_k=p_1p_2\cdots p_k+1$. 求使 f_k 不为素数的最小 k.

***1.50** 证明：若 d，d' 都是非零整数且互相整除，则 $d'=\pm d$.

H 1.51　若 ζ 是一个单位根，证明存在正整数 d 满足 $\zeta^d=1$，且只要 $\zeta^k=1$ 就有 $d\mid k$. 53

H 1.52　证明每个正整数 m 可以表示成 2 的不同幂的和，而且这种表示是唯一的.

1.53　对 $b=2, 3, 4, 5$ 和 20，求 1000 的 b-进位数.

*1.54　**H** (i)证明，若 n 是**无平方因子整数**(即，$n>1$ 且 n 不能被任意素数的平方整除)，则$\sqrt{n}$是无理数.

H (ii)证明$\sqrt[3]{2}$是无理数.

1.55　(i)求 $d=\gcd(12\,327, 2409)$，求整数 s 和 t 使得 $d=12\,327s+2409t$. 并把分数 2409/12 327 表示成既约形式.

(ii)求 $d=\gcd(7563, 526)$，并把 d 表示成 7563 和 526 的线性组合.

(iii)求 $d=\gcd(73\,122, 7\,404\,621)$，并把 d 表示成 73 122 和 7 404 621 的线性组合.

*1.56　设 a，b 都是整数且 $sa+tb=1$，$s, t\in\mathbf{Z}$. 证明 a 和 b 互素.

*1.57　若 $d=(a, b)$，证明 a/d 和 b/d 互素.

***H 1.58**　证明：若$(r, m)=1=(r', m)$，则$(rr', m)=1$.

H 1.59　设 a，b，d 都是整数. 若 $d=sa+tb$，其中 s，t 都是整数，求出无穷多对整数(s_k, t_k)使得 $d=s_ka+t_kb$.

***H 1.60**　证明：若 a，b 互素且都整除整数 n，则它们的积 ab 也整除 n.

***H 1.61**　证明：对任意(可能负的)整数 a 和 b，有$(b, a)=(b-a, a)$.

H 1.62　设 $a>0$，证明 $a(b, c)=(ab, ac)$. [我们必须假设 $a>0$ 以免 $a(b, c)$是负数.]

1.63　证明下面的伪码补充了欧几里得算法.

```
Input : a,b
Output : d
d := b; s := a
WHILE s > 0 DO
   rem := 用 s 除 d 后的余数
   d := s
   s := rem
END WHILE
```

H 1.64　若 F_n 表示斐波那契序列 0，1，1，2，3，5，8，…的第 n 项，证明，对所有 $n\geqslant1$，F_{n+1} 和 F_n 互素.

定义　设 $a_1, a_2, \cdots, a_n$ 都是整数，若整数 c 满足对所有 i 有 $c\mid a_i$，则称 c 是 $a_1, a_2, \cdots, a_n$ 的一个**公因子**. 公因子中最大的那一个记为$(a_1, a_2, \cdots, a_n)$，称为**最大公因子**.

*1.65　(i)证明，若 d 是 $a_1, a_2, \cdots, a_n$ 的最大公因子，则 $d=\sum t_ia_i$，其中 $t_i\in\mathbf{Z}$，$1\leqslant i\leqslant n$.

(ii)证明，若 c 是 $a_1, a_2, \cdots, a_n$ 的一个公因子，则 $c\mid d$.

*1.66　(i)证明$(a, b, c)=(a, (b, c))$.

(ii)计算(120, 168, 328). 54

*1.67　**毕达哥拉斯三元数组**是指由满足

$$a^2+b^2=c^2$$

的正整数 a、b、c 构成的三元数组(a, b, c). 若最大公因子$(a, b, c)=1$，则称这个数组是**本原的**.

(i)考虑复数 $z=q+ip$，其中 $q>p$ 都是正整数. 通过证明 $|z^2|=|z|^2$ 来证明

$$(q^2-p^2, 2qp, q^2+p^2)$$

是毕达哥拉斯三元数组. [我们可以证明每个本原的毕达哥拉斯三元数组(a, b, c)都是这种类型的.]

(ii)证明毕达哥拉斯三元数组(9, 12, 15)(不是本原的)不属于(i)中给出的类型.

(iii)利用计算器可以求出平方根，但是只能显示 8 位数字，求出 q 和 p 来证明

$$(19\,597\,501, 28\,397\,460, 34\,503\,301)$$

是毕达哥拉斯三元数组.

→1.4 算术基本定理

我们在定理 1.2 中已经看到，每个整数 $a\geq 2$ 或是素数，或是素数的积. 现在我们来推广命题 1.14，证明在这样的分解式中每个素数以及它们的次数是由 a 唯一确定的.

→ **定理 1.51（算术基本定理）** *每个整数 $a\geq 2$ 或是素数，或是素数的积. 而且，若 a 有分解式*

$$a = p_1\cdots p_m \quad \text{和} \quad a = q_1\cdots q_n,$$

其中 $p_1, \cdots, p_m, q_1, \cdots, q_n$ 都是素数，则 $n=m$，且对 $q_1, \cdots, q_n$ 重新标下标可使对所有 i 有 $q_i=p_i$.

证明 我们可以假设 $m\geq n$，并对 m 应用归纳法证明.

基础步骤. 若 $m=1$，则 $a=p_1=q_1$，结论显然成立.

归纳步骤. 由等式知 $p_m \mid q_1\cdots q_n$. 又由定理 1.38 即欧几里得引理知，存在 i 满足 $p_m \mid q_i$. 但是 q_i 是素数，除 1 和自身外没有其他正因子，所以 $q_i=p_m$. 重新给下标，我们可假设 $q_n=p_m$，消去后有 $p_1\cdots p_{m-1}=q_1\cdots q_{n-1}$. 由归纳假设知 $n-1=m-1$，且对 $q_1, \cdots, q_{n-1}$ 重排下标
55 可使对所有 i 有 $q_i=p_i$. ■

→ **推论 1.52** *若 $a\geq 2$ 是整数，则存在唯一的相异素数 p_i 和唯一的整数 $e_i>0$ 满足*

$$a = p_1^{e_1}\cdots p_n^{e_n}.$$

证明 只要合并素数分解中的相同项即可. ■

算术基本定理中的唯一性是说，素分解式 $a=p_1^{e_1}\cdots p_n^{e_n}$ 中的指数 $e_1, \cdots, e_n$ 是定义良好的且是由 a 确定的整数. 也就是说，若 $n=p^2q^5r^6$ 且 $n=p^2q^3s^8$，其中 p, q, r, s 是不同的素数，则说 n 的"q 的指数"是没有意义的.

有时允许分解式中有一些零指数是很方便的，这是因为当分解两个整数时可以使用相同的素数. 例如，$168=2^3 3^1 7^1$，$60=2^2 3^1 5^1$ 可重写为 $168=2^3 3^1 5^0 7^1$，$60=2^2 3^1 5^1 7^0$.

推论 1.53 *每个正有理数 $r\neq 1$ 有唯一分解式*

$$r = p_1^{g_1}\cdots p_n^{g_n},$$

其中 p_i 是互异的素数，g_i 是非零整数. 而且 r 是整数当且仅当对所有 i 有 $g_i>0$.

证明 存在正整数 a 和 b 使得 $r=a/b$. 若 $a=p_1^{e_1}\cdots p_n^{e_n}$，$b=p_1^{f_1}\cdots p_n^{f_n}$，则 $r=p_1^{g_1}\cdots p_n^{g_n}$，其中 $g_i=e_i-f_i$(通过允许指数为零，我们可假设两个分解中出现相同的素数). 若 $g_i=0$，则消去 $p_i^{g_i}$ 得要证的分解式.

假设还有另一个分解式

$$r = p_1^{h_1}\cdots p_n^{h_n}$$

(通过允许指数为零，我们又可假设每个分解中出现相同的素数). 如有必要可重排下标，假设对某个 j 有 $g_j\neq h_j$，不妨设 $j=1$，$g_1>h_1$. 因此

$$p_1^{g_1-h_1}p_2^{g_2}\cdots p_n^{g_n}=p_2^{h_2}\cdots p_n^{h_n}.$$

因为某些指数可能为负数，所以这是有理数等式．通过交叉相乘可得到整数等式，其左边含有素数 p_1，而右边不含有 p_1，这与算术基本定理矛盾．

若 r 的分解式中所有指数为正数，则 r 是一些整数的乘积，于是 r 是整数；反之，若 r 是整数，则其素数分解中所有指数为正数． ■ 56

引理 1.54 设正整数 a 和 b 的素数分解式分别为

$$a=p_1^{e_1}\cdots p_n^{e_n},\quad b=p_1^{f_1}\cdots p_n^{f_n},$$

其中 p_1，…，p_n 是相异素数，对所有 i，e_i，$f_i\geqslant 0$．则 $a\mid b$ 当且仅当对所有 i，$e_i\leqslant f_i$．

证明 若对所有 i，$e_i\leqslant f_i$，则 $b=ac$，其中 $c=p_1^{f_1-e_1}\cdots p_n^{f_n-e_n}$．因为 $f_i-e_i\geqslant 0$，$i=1$，…，n，所以由推论 1.53 知 c 是整数．因此 $a\mid b$．

反之，若 $b=ac$，设 c 的素分解式为 $c=p_1^{g_1}\cdots p_n^{g_n}$，$g_i\geqslant 0$，$i=1$，…，$n$．由算术基本定理得 $e_i+g_i=f_i$，$i=1$，…，n，因此对所有 i 有 $f_i-e_i=g_i\geqslant 0$． ■

→ **定义** 设 a，b 都是整数，若整数 m 满足 $a\mid m$ 和 $b\mid m$，则称 m 为 a，b 的一个**公倍数**．若 $a\neq 0$，$b\neq 0$，则 a，b 的**最小公倍数**是指最小的正公倍数；若 a，b 至少有一个为 0，则 a，b 的最小公倍数是 0．a，b 的最小公倍数记为 $\mathrm{lcm}(a, b)$（或简记为 $[a, b]$）．

更一般地，设 a_1，a_2，…，a_n 是整数，$n\geqslant 2$，若整数 m 满足对所有 i 有 $a_i\mid m$，则称 m 为 a_1，a_2，…，a_n 的一个公倍数．若所有 $a_i\neq 0$，则 a_1，a_2，…，a_n 的最小公倍数是指最小的正公倍数；否则，a_1，a_2，…，a_n 的最小公倍数是 0．a_1，a_2，…，a_n 的最小公倍数记为

$$[a_1,a_2,\cdots,a_n].$$

我们现在可以给出最大公因子的一个新的描述．

→ **命题 1.55** 设 $a=p_1^{e_1}\cdots p_n^{e_n}$，$b=p_1^{f_1}\cdots p_n^{f_n}$，其中 p_1，…，p_n 是相异素数，e_i，$f_i\geqslant 0$，$i=1$，…，n．定义

$$m_i=\min\{e_i,f_i\},\quad M_i=\max\{e_i,f_i\}.$$

则

$$\gcd(a,b)=p_1^{m_1}\cdots p_n^{m_n},\quad \mathrm{lcm}(a,b)=p_1^{M_1}\cdots p_n^{M_n}.$$

证明 设 $d=p_1^{m_1}\cdots p_n^{m_n}$．由引理 1.54 知 d 是 a 和 b 的（正）公因子．而且，若 c 是 a 和 b 的任一（正）公因子，则 $c=p_1^{g_1}\cdots p_n^{g_n}$，$0\leqslant g_i\leqslant\min\{e_i, f_i\}=m_i$，$i=1$，…，$n$，因此 $c\mid d$．

类似的讨论可知，$D=p_1^{M_1}\cdots p_n^{M_n}$ 是 a 和 b 的公倍数，且可以整除 a 和 b 的其他任意公倍数． ■

对较小的数 a 和 b，在计算它们的最大公因子时，利用它们的素数分解比利用欧几里得算法更有效．例如，$168=2^3 3^1 5^0 7^1$，$60=2^2 3^1 5^1 7^0$，所以 $(168, 60)=2^2 3^1 5^0 7^0=12$，$[168, 60]=2^3 3^1 5^1 7^1=840$．我们在介绍欧几里得算法时提到过，求一个较大整数的素分解式是非常困难的． 57

命题 1.56 若 a，b 都是正整数，则

$$\mathrm{lcm}(a,b)\gcd(a,b)=ab.$$

证明 我们可以利用恒等式

$$m_i + M_i = e_i + f_i,$$

由命题 1.55 得证，其中 $m_i=\min\{e_i, f_i\}$，$M_i=\max\{e_i, f_i\}$. ■

当然这个命题使得我们可以用 $ab/(a, b)$ 计算最小公倍数.

习题

H 1.68 判断对错并说明理由.

(i) $|2^{19}-3^{12}|<\frac{1}{2}$.

(ii) 若 $r=p_1^{g_1}\cdots p_n^{g_n}$，其中 p_i 是相异素数，且 g_i 都是整数，则 r 是一个整数当且仅当所有 g_i 都是非负的.

(iii) 最小公倍数 $[2^3\cdot 3^2\cdot 5\cdot 7^2, 3^3\cdot 5\cdot 13]=2^3\cdot 3^5\cdot 5^2\cdot 7^2\cdot 13/45$.

(iv) 若 a，b 都是正整数且不互素，则存在素数 p 满足 $p\mid a$ 和 $p\mid b$.

(v) 若 a，b 互素，则 $(a^2, b^2)=1$.

1.69 (i) 用素分解式求 gcd(210, 48).

(ii) 求 gcd(1234, 5678).

*1.70 (i) 证明整数 $m\geqslant 2$ 是一个完全平方数当且仅当它的每个素因子出现偶数次.

H (ii) 证明：若 m 是一个正整数且 $\sqrt{m}$ 是有理数，则 m 是一个完全平方数. 由此知若 m 不是一个完全平方数，则 $\sqrt{m}$ 是无理数.

H 1.71 设 a，b 都是正整数满足 $(a, b)=1$，若 ab 是平方数，证明 a 和 b 都是平方数.

*H 1.72 设 $n=p^r m$，其中 p 是素数但不能整除整数 $m\geqslant 1$. 证明 $p\nmid\binom{n}{p^r}$.

定义 设 p 是一个素数，定义有理数 a 的 **p-进位范数**如下：若 $a\neq 0$，则 $a=\pm p^e p_1^{e_1}\cdots p_n^{e_n}$，其中 p，p_1，…，p_n 是互异素数，并令 $\|a\|_p=p^{-e}$；若 $a=0$，则令 $\|0\|_p=0$. 定义 **p-进位度量**为 $\delta_p(a, b)=\|a-b\|_p$.

*1.73 (i) 对所有有理数 a 和 b，证明

$$\|ab\|_p=\|a\|_p\|b\|_p,\quad \|a+b\|_p\leqslant\max\{\|a\|_p, \|b\|_p\}.$$

(ii) 对所有有理数 a，b，证明 $\delta_p(a, b)\geqslant 0$，以及 $\delta_p(a, b)=0$ 当且仅当 $a=b$.

(iii) 对所有有理数 a，b，证明 $\delta_p(a, b)=\delta_p(b, a)$.

(iv) 对所有有理数 a，b，c，证明 $\delta_p(a, b)\leqslant\delta_p(a, c)+\delta_p(c, b)$.

(v) 若 a，b 都是整数且 $p^n\mid(a-b)$，则 $\delta_p(a, b)\leqslant p^{-n}$.（因此，若 $a-b$ 可被 p 的一个“很大”幂整除，

58 则 a 和 b 是“接近的”.）

1.74 设 $a, b\in\mathbb{Z}$. 证明，若 $\delta_p(a, b)\leqslant p^{-n}$，则 a 和 b 有相同的前 n 个 p-进位数 d_0，…，d_{n-1}.

1.75 证明一个整数 $M\geqslant 0$ 是 a_1，a_2，…，a_n 的最小公倍数当且仅当它是 a_1，a_2，…，a_n 的一个公倍数且整除任意其他公倍数.

*1.76 H (i) 不用算术基本定理，给出命题 1.56 即 $[a, b](a, b)=|ab|$ 的另一个证明.

(ii) 求 [1371, 123].

→1.5 同余

当开始学习长除法的时候，我们强调商 q，而余数 r 仅仅是留下的部分. 现在我们在观点上有一个转变：我们将对给定的整数 b 是否是整数 a 的倍数感兴趣，但是对 b 是哪个整数的倍数不这么感兴趣. 因此，从现在起，我们将强调余数.

如果整数 a 和 b 都是偶数，或者都是奇数，则称它们**同奇偶性**. 可以断言：a 和 b 同奇偶性当且仅当 $a-b$ 是偶数. 当 a，b 都是偶数时，这个断言显然是正确的；当 a，b 都是奇数时，令 $a=2m+1$，$b=2n+1$，则 $a-b=2(m-n)$是偶数. 反之，若 $a-b$ 是偶数，则 a 和 b 不可能一个为偶数，而另一个为奇数，否则 $a-b$ 是奇数. 下面的定义推广了奇偶性的概念，让任何一个正整数 m 都起到了 2 的作用.

→ **定义** 给定整数 $m\geqslant 0$，若对整数 a 和 b 有 $m\mid(a-b)$，则称 a，b **模** m **同余**，记为

$$a\equiv b(\mathrm{mod}\ m)\quad 或\quad a\equiv b \bmod m.$$

通常，人们假定模 $m\geqslant 2$，因为 $m=0$ 和 $m=1$ 的情形无法引起人们多大兴趣：若 a，b 是整数，则 $a\equiv b(\mathrm{mod}\ 0)$当且仅当 $0\mid(a-b)$，即 $a=b$，因此关于模 0 的同余是普通等式；对每对整数 a 和 b，因为 $1\mid(a-b)$恒成立，所以同余式 $a\equiv b(\mathrm{mod}\ 1)$恒成立. 因而任何两个整数模 1 同余.

词语模“modulo(模)”通常缩写为“mod”. 这个词的拉丁词根的意思是“一个度量标准”. 因此术语“模的单位”今天用在建筑学中：选定一个固定长度 m，不妨设为 $m=1$ 英尺，按此规定可使得每扇窗，每扇门和每堵墙等等的尺寸都是 m 的整数倍.

设 a 和 b 是正整数，则 $a\equiv b(\mathrm{mod}\ 10)$当且仅当它们有相同的末尾数字. 一般地，$a\equiv b(\mathrm{mod}\ 10^n)$当且仅当它们有相同的末尾 n 个数字. 例如，$526\equiv 1926(\mathrm{mod}\ 100)$. 59

伦敦时间比芝加哥时间迟 6 个小时. 若芝加哥时间是早上 10：00，那么伦敦时间是多少呢？因为时钟以 12 小时为一周期，所以这实际上是一个关于模 12 同余的问题. 为解决它，注意到

$$10+6=16\equiv 4(\mathrm{mod}\ 12),$$

所以伦敦时间是下午 4：00.

下面的定理表明模 m 同余有着和相等关系非常类似的性质.

→ **命题 1.57** 给定整数 $m\geqslant 0$，则对所有整数 a，b，c，有

(i) $a\equiv a(\mathrm{mod}\ m)$；

(ii) 若 $a\equiv b(\mathrm{mod}\ m)$，则 $b\equiv a(\mathrm{mod}\ m)$；

(iii) 若 $a\equiv b(\mathrm{mod}\ m)$，$b\equiv c(\mathrm{mod}\ m)$，则 $a\equiv c(\mathrm{mod}\ m)$.

注 (i)是指同余有**自反性**，(ii)是指同余有**对称性**，(iii)是指同余有**传递性**.

证明 (i)由于 $m\mid(a-a)=0$，所以 $a\equiv a(\mathrm{mod}\ m)$.

(ii)若 $m\mid(a-b)$，则 $m\mid-(a-b)=b-a$，因此 $b\equiv a(\mathrm{mod}\ m)$.

(iii)若 $m\mid(a-b)$，$m\mid(b-c)$，则 $m\mid[(a-b)+(b-c)]=a-c$，因此 $a\equiv c(\mathrm{mod}\ m)$. ■

下面推广我们观察到的事实 $a\equiv 0(\mathrm{mod}\ m)$当且仅当 $m\mid a$.

→ **命题 1.58** 给定整数 $m\geqslant 0$.

(i) 若 $a=qm+r$，则 $a\equiv r(\mathrm{mod}\ m)$.

(ii) 若 $0\leqslant r'<r<m$，则 $r\not\equiv r'(\mathrm{mod}\ m)$，即 r 和 r' 模 m 不同余.

(iii) $a\equiv b(\mathrm{mod}\ m)$当且仅当 a 和 b 被 m 除后余数相同.

证明 (i)等式 $a-r=qm$ 表明 $m\mid(a-r)$.

(ii)若 $r\equiv r'\ (\mathrm{mod}\ m)$，则 $m\mid(r-r')$且 $m\leqslant r-r'$. 但 $r-r'\leqslant r<m$，矛盾.

(iii)若 $a=qm+r$，$b=q'm+r'$，其中 $0\leqslant r<m$，$0\leqslant r'<m$，则 $a-b=(q-q')m+(r-r')$，即

60 $$a-b\equiv r-r'(\mathrm{mod}\ m).$$

因此，若 $a\equiv b(\mathrm{mod}\ m)$，则 $a-b\equiv 0(\mathrm{mod}\ m)$，则 $r-r'\equiv 0(\mathrm{mod}\ m)$，$r\equiv r'(\mathrm{mod}\ m)$. 由(ii)知 $r=r'$.

反之，若 $r=r'$，则 $a=qm+r$，$b=q'm+r$，所以 $a-b=(q-q')m$，这样 $a\equiv b(\mathrm{mod}\ m)$. ■

→ **推论 1.59** 给定 $m\geqslant 2$，则每个整数 a 模 m 同余于 0，1，…，$m-1$ 中的某一个.

证明 由除法算式知 $a\equiv r(\mathrm{mod}\ m)$，其中 $0\leqslant r<m$，即 r 是 0，1，…，$m-1$ 中的某一个. 若 a 与这列数中的两个整数同余，不妨设为 r 和 r'，则 $r\equiv r'\ (\mathrm{mod}\ m)$，此与命题 1.58 中的(ii)矛盾. 因此，$a$ 与这列数中唯一的 r 同余. ■

我们知道任何整数 a 或为偶数或为奇数，即 a 有形式 $2k$ 或 $1+2k$. 可以看出，若 $m\geqslant 2$，则整数 a 恰有 $0+km$，$1+km$，$2+km$，…，$(m-1)+km$ 之中的某一种形式. 这样我们将 $m=2$的奇偶二分法推广到了 $m\geqslant 2$. 注意，我们是怎样继续将注意力集中在除法算式的余数上，而不是在商上的.

同余与加法和乘法是相容的.

→ **命题 1.60** 给定整数 $m\geqslant 0$.

(i)若 $a_i\equiv a_i'(\mathrm{mod}\ m)$，$i=1$，2，…，$n$，则
$$a_1+\cdots+a_n\equiv a'_1+\cdots+a'_n(\mathrm{mod}\ m).$$
特别地，若 $a\equiv a'(\mathrm{mod}\ m)$，$b\equiv b'(\mathrm{mod}\ m)$，则
$$a+b\equiv a'+b'(\mathrm{mod}\ m).$$
(ii)若 $a_i\equiv a_i'(\mathrm{mod}\ m)$，$i=1$，2，…，$n$，则
$$a_1\cdots a_n\equiv a'_1\cdots a'_n(\mathrm{mod}\ m).$$
特别地，若 $a\equiv a'(\mathrm{mod}\ m)$，$b\equiv b'(\mathrm{mod}\ m)$，则
$$ab\equiv a'b'(\mathrm{mod}\ m).$$
(iii)若 $a\equiv b(\mathrm{mod}\ m)$，则对所有 $n\geqslant 1$，$a^n\equiv b^n(\mathrm{mod}\ m)$.

证明 (i)对 $n\geqslant 2$ 用归纳法证明. 对基础步骤，若 $m\mid(a-a')$，$m\mid(b-b')$，则 $m\mid[(a-a')+(b-b')]=(a+b)-(a'+b')$. 因此 $a+b\equiv a'+b'(\mathrm{mod}\ m)$. 归纳步骤的证明是常

61 规的.

(ii)对 $n\geqslant 2$ 用归纳法证明. 对基础步骤，我们必须证明若 $m\mid(a-a')$且 $m\mid(b-b')$，则 $m\mid(ab-a'b')$，而这能由下面的等式得到
$$\begin{aligned}ab-a'b'&=(ab-a'b)+(a'b-a'b')\\&=(a-a')b+a'(b-b').\end{aligned}$$
因此，$ab\equiv a'b'(\mathrm{mod}\ m)$. 归纳步骤的证明是常规的.

(iii)在(ii)中对所有 i 令 $a_i=a$，$a_i'=b$，即可得证. ■

我们证明除法算式时给出了一个警告，现在让我们重述一下. 通常，一个数和它的相反数被数 m 所除得到的余数不同. 例如，$60=7\cdot 8+4$，$-60=7\cdot(-9)+3$. 根据同余，

$$60\equiv 4(\bmod 7) \quad 而 \quad -60\equiv 3(\bmod 7).$$

根据命题 1.58(i)，若 b 被 m 除后余数是 r，而 $-b$ 被 m 除后余数是 s，则 $b\equiv r(\bmod m)$，$-b\equiv s(\bmod m)$. 因此由命题 1.60(i)知

$$r+s\equiv b-b\equiv 0(\bmod m).$$

因此，若 b 不是 m 的倍数，则 $r\neq 0$，$s\neq 0$，又因为 $0\leqslant r$，$s<m$，所以 $r+s=m$. 例如，用 7 去除 60 和 -60 所得余数分别是 4 和 3. 若 a 和 $-a$ 被 m 除有相同的余数 r，则 $-r\equiv r(\bmod m)$，即 $2r\equiv 0(\bmod m)$. 习题 1.84 要求我们证明这个同余式.

下面这个例子展示了如何使用同余方法. 每一种情形的主要思想都是用数的余数代替数来解决问题.

例 1.61 (i)若 $a\in\mathbb{Z}$，则 $a^2\equiv 0$，1 或 $4(\bmod 8)$.

若 a 是整数，则 $a\equiv r(\bmod 8)$，其中 $0\leqslant r\leqslant 7$. 另外，由命题 1.60(iii)知 $a^2\equiv r^2(\bmod 8)$，所以只须看看这些余数的平方. 在表 1-1 中我们看到，一个完全平方数被 8 除后的余数只能是 0，1 或 4.

表 1-1 平方数 mod 8

r	0	1	2	3	4	5	6	7
r^2	0	1	4	9	16	25	36	49
$r^2(\bmod 8)$	0	1	4	1	0	1	4	1

62

(ii)$n=1\,003\,456\,789$ 不是完全平方数.

由于 $1000=8\cdot 125$，我们有 $1000\equiv 0(\bmod 8)$，所以

$$1\,003\,456\,789=1\,003\,456\cdot 1000+789\equiv 789(\bmod 8).$$

用 8 除 789 得余数 5，即 $n\equiv 5(\bmod 8)$. 但是，若 n 是完全平方数，则 $n\equiv 0$，1 或 $4(\bmod 8)$.

(iii)若 m，n 都是正整数，则没有形如 3^m+3^n+1 的完全平方数.

让我们看看模 8 的余数. 由于 $3^2=9\equiv 1(\bmod 8)$，所以可计算 $3^m(\bmod 8)$如下：若 $m=2k$，则 $3^m=3^{2k}=9^k\equiv 1(\bmod 8)$；若 $m=2k+1$，则 $3^m=3^{2k+1}=9^k\cdot 3\equiv 3(\bmod 8)$. 因此，

$$3^m\equiv\begin{cases}1(\bmod 8) & m=2k;\\ 3(\bmod 8) & m=2k+1.\end{cases}$$

用被 8 除后的余数代替这些数，我们得到 3^m+3^n+1 的余数有如下几种可能：

$$3+1+1\equiv 5(\bmod 8)$$
$$3+3+1\equiv 7(\bmod 8)$$
$$1+1+1\equiv 3(\bmod 8)$$
$$1+3+1\equiv 5(\bmod 8).$$

没有余数是 0，1 或 4 的情况，所以由(i)知形如 3^m+3^n+1 的数不是完全平方数. ◀

每个正整数模 3 同余于 0，1 或 2. 因此，若 $p\neq 3$ 是一个素数，则或者 $p\equiv 1(\bmod 3)$，或者 $p\equiv 2(\bmod 3)$. 例如，7，13 和 19 模 3 同余于 1，而 2，5，11 和 17 模 3 同余于 2. 下面这

个定理说明一个事实：对一个定理的证明进行调整后可以用来证明另一个定理.

命题 1.62 存在无穷多个素数 p 满足 $p\equiv 2(\bmod 3)$.

注 这个命题是漂亮的狄利克雷(Dirichlet)定理的特殊情形，这个定理是：若 a，$b\in \mathbb{N}$ 且互素，则存在无穷多个具有形式 $a+bn$ 的素数. 在这个命题中，我们证明存在无穷多个具有形式 $2+3n$ 的素数. 虽然这个特殊情形的证明不难，但是狄利克雷定理的
63 证明用到了复分析知识且很深奥.

证明 我们模仿欧几里得证明存在无穷多个素数的方法. 假设只有有限多个素数模 3 同余于 2，设它们是 p_1，…，p_s. 考虑数

$$m = 1 + p_1^2 \cdots p_s^2.$$

由 $p_i\equiv 2(\bmod 3)$可推出 $p_i^2\equiv 4\equiv 1(\bmod 3)$，因此 $p_1^2\cdots p_s^2\equiv 1(\bmod 3)$，所以 $m\equiv 1+1=2(\bmod 3)$. 因为对所有 i 有 $m>p_i$，所以数 m 不是素数，这是因为它不是 p_i 中的某一个. 实际上 p_i 都不整除 m：若我们定义 $Q_i=p_1^2\cdots p_{i-1}^2 p_i p_{i+1}^2\cdots p_s^2$，则除法算式的唯一性部分和等式 $m=p_iQ_i+1$ 一起表明，m 被 p_i 除后余数为 1. 因此，m 的素分解式是 $m=q_1\cdots q_t$，其中对每个 j，或者$q_j\equiv 1(\bmod 3)$或者 $q_j\equiv 0(\bmod 3)$. 因此 $m=q_1\cdots q_t\equiv 0(\bmod 3)$，或 $m=q_1\cdots q_t\equiv 1(\bmod 3)$，这与 $m\equiv 2(\bmod 3)$矛盾. ■

下面这个结果展示了同余是怎样简化一些复杂表达式的.

→ **命题 1.63** 若 p 是素数，a，b 都是整数，则

$$(a+b)^p \equiv a^p + b^p (\bmod p).$$

证明 由二项式定理知

$$(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1}\binom{p}{r}a^{p-r}b^r.$$

但由命题 1.39 知$\binom{p}{r}\equiv 0(\bmod p)$，$0<r<p$，所以由命题 1.60(i)有$(a+b)^p\equiv a^p+b^p(\bmod p)$. ■

→ **定理 1.64 (费马定理)** (i)若 p 是素数，则对每个 $a\in \mathbb{Z}$ 有

$$a^p \equiv a(\bmod p).$$

(ii)若 p 是素数，则对每个 $a\in \mathbb{Z}$ 和每个整数 $k\geqslant 1$ 有

64
$$a^{p^k} \equiv a(\bmod p).$$

证明 (i)首先假设 $a\geqslant 0$. 以下对 a 用归纳法. 基础步骤 $a=0$ 是显然成立的. 对于归纳步骤，由命题 1.63 知

$$(a+1)^p \equiv a^p + 1(\bmod p).$$

由归纳假设得 $a^p\equiv a(\bmod p)$，所以$(a+1)^p\equiv a^p+1\equiv a+1(\bmod p)$.

现考虑$-a$，其中 $a\geqslant 0$. 若 $p=2$，则$-a\equiv a$，因而$(-a)^2=a^2\equiv a\equiv -a(\bmod 2)$. 若 p 是奇素数，则$(-a)^p=(-1)^p a^p\equiv(-1)^p a\equiv -a(\bmod p)$.

(ii)直接对 $k\geqslant 1$ 用归纳法可得证，其基础步骤就是(i). ■

推论 1.65 正整数 n 可被 3(或 9)整除，当且仅当其(十进制)各位数字之和可被 3(或 9)

整除.

证明 若 n 的十进制形式为 $d_k \cdots d_1 d_0$，则

$$n = d_k 10^k + \cdots + d_1 10 + d_0.$$

由于 $10 \equiv 1 \pmod 3$，所以由命题 1.60(iii)知对所有 i，$10^i \equiv 1^i = 1 \pmod 3$，因此由命题 1.60(i)知 $n \equiv d_k + \cdots + d_1 + d_0 \pmod 3$. 因此 n 可被 3 整除当且仅当 $n \equiv 0 \pmod 3$ 当且仅当 $d_k + \cdots + d_1 + d_0 \equiv 0 \pmod 3$.

因为 $10 \equiv 1 \pmod 9$，所以用相同的证法可以证明关于 9 的结论. ■

例 1.66 (弃九法) 在正整数 n 的十进制数字上定义两种运算.

(i)除去所有的 9 或任意一组总和为 9 的数字.

(ii)把所有数字都加起来.

原因很明显，通过重复(i)和(ii)这两种运算来改变一个整数的方法称为**弃九法**. 若 n 至少有两个数字，则两种运算都可用一个严格小于 n 的整数代替 n 进行运算. 因此，弃九法最终给出单个的数字，不妨设为 $r(n)$，满足 $0 \leqslant r(n) < 9$(若这个数字是 9，则第一个运算用 0 代替它). $r(n)$可能存在很多值.

例如，(i)改变 5 261 934 为 526 134 为 2613(因为 $5+4=9$)为 21(因为 $6+3=9$)为 $1+2=3$. 因为 $2+3+4=9$，所以我们也可以是这样：5 261 934→526 134→561→21→3. 注意到弃九法可以很快做完.

推论 1.65 表明一个整数 n 的数字总和模 9 同余于 n. 因此，对整数 n 应用(ii)不能改变其模 9 的余数. 若有个数字是 9，或者某组数字之和是 9，则像在运算(i)中那样去掉它们，从而得到一个模 9 同余于 n 的整数. 我们由此得 $r(n) \equiv n \pmod 9$. 另外，因为 $0 \leqslant r(n) < 9$，所以推论 1.59 表明，整数 n 不依赖所用的运算. 简言之，$r(n)$是被 9 除后的余数. 65

这里有检验算术错误的簿记[⊖]诀窍. 我们用弃九法检验等式(12 345+5 261 944)1776=9 367 119 504是否正确. 现在 $r(12\,345)=6$，$r(5\,261\,934)=3$，正如我们在上面所看到的，而且 $r(1776)=3$. 根据命题 1.60，$r([12\,345+5\,261\,944]\times 1776)=r([6+3]\times 3)=0$. 因为 $r(9\,367\,119\,504)=0$，所以两边有相同的余数，计算通过了弃九法的检验(假设两边不同，则出了错误). 不幸的是，这个诀窍不能保证计算的正确性. 例如，若 n'是通过将 n 交换两个数字而得到的，则 $r(n')=r(n)$. 所以颠倒数字不能被弃九法检测出来. ◀

推论 1.67 *设 p 是素数，n 是正整数. 若 $m \geqslant 0$，且 $\sum(m)$ 是 m 的 p-进位数之和，则*

$$n^m \equiv n^{\sum(m)} \pmod p.$$

证明 设 $m = d_k p^k + \cdots + d_1 p + d_0$ 是 m 的以 p 为底数的表示式. 由费马定理即定理 1.64(ii)知，对所有 i 有 $n^{p^i} \equiv n \pmod p$，因此 $n^{d_i p^i} = (n^{d_i})^{p^i} \equiv n^{d_i} \pmod p$. 因此

⊖ 单词"簿记(bookkeeper)"有三个连续双写的字母：oo，kk，ee. 这里还有一个有六个连续双写字母的单词. 在马德里的动物园中，有一只名叫 Ramon 的浣熊(raccoon)，它是最吸引游客的动物. Ramon 会跳舞，古典芭蕾和弗拉门哥舞都会. 由于它吸引了太多的游客使笼子周围十分拥挤，因此动物园给了它一个属于自己的笼子. 但是，Ramon 需要一个能让它远离游客赞美的私人角落来缓解演出带来的压力. 于是动物园雇佣了一个特殊的服务员来满足 Ramon 的要求，这个人被称作 raccoonnookkeeper.

$$\begin{aligned} n^m &= n^{d_k p^k + \cdots + d_1 p + d_0} \\ &= n^{d_k p^k} n^{d_{k-1} p^{k-1}} \cdots n^{d_1 p} n^{d_0} \\ &\equiv n^{d_k} n^{d_{k-1}} \cdots n^{d_1} n^{d_0} \pmod p \\ &\equiv n^{d_k + \cdots + d_1 + d_0} \pmod p \\ &\equiv n^{\Sigma(m)} \pmod p. \end{aligned}$$ ■

例 1.68 $3^{12\,345}$被 7 除后余数是多少？由例 1.48 知 12 345 的 7-进位数是 50 664. 因此 $3^{12\,345} \equiv 3^{21} \pmod 7$（因为 $5+0+6+6+4=21$）. 而 21 的 7-进位数是 30（因为 $21=3\times7$），所以
66 $3^{21} \equiv 3^3 \pmod 7$（因为 $3+0=3$）. 我们得到 $3^{12\,345} \equiv 3^3 = 27 \equiv 6 \pmod 7$. ◀

→ **定理 1.69** 若$(a, m)=1$，则对每个整数 b，同余式

$$ax \equiv b \pmod m$$

对 x 总是有解的. 实际上 $x=sb$，其中 $sa\equiv 1 \pmod m$. 而且，任何两个解对模 m 同余.

注 习题 1.89 中考虑了$(a, m)\neq 1$ 的情形.

证明 因为$(a, m)=1$，所以存在整数 s 满足 $as\equiv 1 \pmod m$（因为存在线性组合 $1=sa+tm$）. 于是，$b=sab+tmb$，$asb\equiv b \pmod m$，所以 $x=sb$ 是一个解. [注意：命题 1.58(i)允许我们取 s 满足 $1\leqslant s<m$.]

若 y 是另一个解，则 $ax\equiv ay \pmod m$，所以 $m \mid a(x-y)$. 由于$(a, m)=1$，由推论 1.40 知 $m \mid (x-y)$，即 $x\equiv y \pmod m$. ■

→ **推论 1.70** 若 p 是素数且 $p \nmid a$，则 $ax\equiv b \pmod p$ 总是有解.

证明 由于 p 是素数且 $p \nmid a$，所以$(a, p)=1$. ■

例 1.71 当$(a, m)=1$ 时，定理 1.69 是说 $ax\equiv b \pmod m$ 的解正好是那些形如 $sb+km$ 的整数，$k\in\mathbb{Z}$，其中 $sa\equiv 1 \pmod m$，即存在整数 t 使得 $sa+tm=1$. 因此，s 总是可以通过欧几里得算法找到的. 但是，当 m 很小时，通过依次试验 $ra=2a, 3a, \cdots, (m-1)a$，容易找到这样的整数 s，每一步都检验是否有 $ra\equiv 1 \pmod m$.

例如，求

$$2x \equiv 9 \pmod{13}$$

的所有解. 考虑 $2\cdot 2, 3\cdot 2, 4\cdot 2, \cdots \pmod{13}$，很快得到 $7\times 2=14\equiv 1 \pmod{13}$，即 $s=7$，$x=7\cdot 9=63\equiv 11 \pmod{13}$，因此

$$x \equiv 11 \pmod{13},$$

且解是$\cdots, -15, -2, 11, 24, \cdots$. ◀

例 1.72 求 $51x\equiv 10 \pmod{94}$ 的所有解.

因为 94 很大，所以若像例 1.71 那样求满足 $51s\equiv 1 \pmod{94}$ 的整数 s 是很烦琐的. 由欧几里得算法得 $1=-35\cdot 51+19\cdot 94$，所以 $s=59$，因为 $59\equiv -35 \pmod{94}$. 解是由所有满足
67 $x\equiv 59\times 10 \pmod{94}$ 的整数构成，即形如 $590+94k$ 的数. ◀

在中国古代的手稿中就解决了以互素数为模的同余方程组解的问题.

→ **定理 1.73（中国剩余定理）** 设整数 m 与 m' 互素，则两个同余方程

$$x\equiv b \pmod m$$

$$x \equiv b'(\mathrm{mod}\ m')$$

有公共解，且任何两个解对模 mm' 同余.

证明　第一个同余方程的解具有形式 $x=b+km$，k 为整数. 因此，我们必须找到 k 使得 $b+km\equiv b'(\mathrm{mod}\ m')$，即 $km\equiv b'-b(\mathrm{mod}\ m')$. 但是，因为 $(m, m')=1$，所以由定理 1.69 可立即证得这样的整数 k 确实存在.

若 y 是另一个公共解，则 m 和 m' 都整除 $x-y$，由习题 1.60 知 $mm' \mid (x-y)$，所以 $x\equiv y(\mathrm{mod}\ mm')$. ■

例 1.74　求同余方程组

$$x\equiv 7(\mathrm{mod}\ 8)$$
$$x\equiv 11(\mathrm{mod}\ 15).$$

的所有解. 第一个同余方程的每个解有形式

$$x = 7 + 8k,$$

k 为整数. 因为 $x=7+8k\equiv 11(\mathrm{mod}\ 15)$，所以

$$8k \equiv 4(\mathrm{mod}\ 15).$$

但是 $2\cdot 8=16\equiv 1(\mathrm{mod}\ 15)$，所以用 2 乘得

$$16k \equiv k \equiv 8(\mathrm{mod}\ 15).$$

我们得到 $x=7+8\cdot 8=71$ 是一个解，且中国剩余定理是说每个解有形式 $71+120n$，$n\in\mathbf{Z}$. ◀

例 1.75　解同余方程组

$$x\equiv 2(\mathrm{mod}\ 5)$$
$$3x\equiv 5(\mathrm{mod}\ 13).$$

68

第一个同余方程的解具有形式 $x=5k+2$，$k\in\mathbf{Z}$，代入到第二个同余方程得

$$3(5k+2)\equiv 5(\mathrm{mod}\ 13).$$

因此，

$$15k+6\equiv 5(\mathrm{mod}\ 13)$$
$$2k\equiv -1(\mathrm{mod}\ 13).$$

因为 $7\times 2\equiv 1(\mathrm{mod}\ 13)$，所以乘以 7 得

$$k\equiv -7\equiv 6(\mathrm{mod}\ 13).$$

由中国剩余定理知同余方程组的解 x 具有形式

$$x\equiv 5k+2\equiv 5\cdot 6+2 = 32(\mathrm{mod}\ 65);$$

即，解是

$$\cdots, -98, -33, 32, 97, 162, \cdots.$$ ◀

若我们没有假设 m 和 m' 互素，则对一个线性系统可能不存在解. 例如，若 $m=m'>1$，则除法算式中余数的唯一性表明，同余方程组

$$x\equiv 0(\mathrm{mod}\ m)$$
$$x\equiv 1(\mathrm{mod}\ m).$$

没有解.

命题 1.76 设 $d=(m, m')$，则系统

$$x \equiv b(\bmod m)$$
$$x \equiv b'(\bmod m').$$

有解当且仅当 $b\equiv b'(\bmod d)$.

注 记住 $b\equiv b'(\bmod 1)$永远成立.

证明 若 $h\equiv b(\bmod m)$，$h\equiv b'(\bmod m')$，则 $m \mid (h-b)$，$m' \mid (h-b')$. 因为 d 是 m 和 m'的一个公因子，所以 $d \mid (h-b)$，$d \mid (h-b')$. 因为$(h-b')-(h-b)=b-b'$，所以 $d \mid (b-b')$，所以 $b\equiv b'(\bmod d)$.

反之，假设 $b\equiv b'(\bmod d)$，则存在整数 k 满足 $b'=b+kd$. 若 $m=dc$，$m'=dc'$，则根据习
69 题 1.57 有$(c, c')=1$. 因此，存在整数 s 和 t 使得 $1=sc+tc'$. 定义 $h=b'sc+btc'$. 现在

$$\begin{aligned} h &= b'sc + btc' \\ &= (b+kd)sc + btc' \\ &= b(sc+tc') + kdsc \\ &= b + ksm \\ &\equiv b(\bmod m). \end{aligned}$$

用 $b'-kd$ 替代 b，类似的讨论得 $h\equiv b'(\bmod m')$. ■

习题 1.96 要求我们证明，给定命题 1.76 的前提条件，则任意两个解模 ℓ 同余，其中 $\ell=\operatorname{lcm}\{m, m'\}$.

例 1.77 解线性系统

$$x \equiv 1(\bmod 6)$$
$$x \equiv 4(\bmod 15).$$

这里，$m=6$，$m'=15$，$d=3$，$c=2$，$c'=5$，$s=3$，$t=-1$. 因为 $1\equiv 4(\bmod 3)$，所以可应用命题 1.76. 定义

$$h = 4\times 3\times 2+1\times(-1)\times 5 = 19.$$

我们检验 $19\equiv 1(\bmod 6)$和 $19\equiv 4(\bmod 15)$. 因为 $\operatorname{lcm}\{6, 15\}=30$，所以解是…，$-41$，$-11$，19，49，79，…. ◀

例 1.78（玛雅人的日历） 只要有循环就会产生同余. 例如，假设我们选择某个特殊的星期日作为零时间，然后列举从这天之后的所有日期，则每个日期对应一个整数，若是零时间之前的日期则对应负数. 现给定两个日期 t_1 和 t_2，我们求两者之间相隔的天数 $x=t_2-t_1$. 若 t_1 是星期四，t_2 是星期二，则 $t_1\equiv 4(\bmod 7)$，$t_2\equiv 2(\bmod 7)$，所以 $x=t_2-t_1=-2\equiv 5(\bmod 7)$，因此 $x=7k+5$，k 为整数.

大约 2500 年以前，中美洲和墨西哥的玛雅人发明了三种日历（每一种日历有不同的用途）. 其中称为卓尔金（tzolkin）的宗教日历包含 20 个“月”，每个“月”有 13 天（所以在卓尔金历中一“年”有 260 天）. 其月份为

1. Imix	2. Ik	3. Akbal	4. Kan
5. Chicchan	6. Cimi	7. Manik	8. Lamat

9. Muluc	10. Oc	11. Chuen	12. Eb
13. Ben	14. Ix	15. Men	16. Cib
17. Caban	18. Etznab	19. Cauac	20. Ahau

70

让我们用一个有序对$\{m, d\}$来描述卓尔金历中的一个日期，其中$1 \leqslant m \leqslant 20$，$1 \leqslant d \leqslant 13$（因此，$m$表示月份，$d$表示天）。玛雅人不是用我们所用的列举方法（Imix 1之后是Imix 2，然后是Imix 3，等等），而是让月和日同时循环，即日子按以下规律推移：

$$\text{Imix } 1, \text{Ik } 2, \text{Akbal } 3, \cdots, \text{Ben } 13, \text{Ix } 1, \text{Men } 2, \cdots,$$
$$\text{Cauac } 6, \text{Ahau } 7, \text{Imix } 8, \text{Ik } 9, \cdots$$

现在我们要问Oc 11和Etznab 5之间相隔多少天．一般地，让我们找出从卓尔金历中$\{m, d\}$到卓尔金历$\{m', d'\}$之间相隔的天数x．正如我们在这个例子一开始所说的，由日子的循环得到同余

$$x \equiv d' - d \pmod{13}$$

（例如，Imix 1和Ix 1之间有13天，这里$x \equiv 0 \pmod{13}$），而由月的循环得到同余

$$x \equiv m' - m \pmod{20}$$

（例如，Imix 1和Imix 8之间有20天，这里$x \equiv 0 \pmod{20}$）．为了回答一开始的问题，让Oc 11对应有序对$\{10, 11\}$，Etznab 5对应$\{18, 5\}$（因为$5-11=-6$，$18-10=8$）．此时联立的同余方程组是

$$x \equiv -6 \pmod{13}$$
$$x \equiv 8 \pmod{20}.$$

由于$(13, 20)=1$，我们可以像中国剩余定理的证明那样来解决这个问题．由第一个同余得

$$x = 13k - 6,$$

由第二个得

$$13k - 6 \equiv 8 \pmod{20},$$

即

$$13k \equiv 14 \pmod{20}.$$

因为$13 \times 17 = 221 \equiv 1 \pmod{20}$，⊖所以$k \equiv 17 \times 14 \pmod{20}$，即

$$k \equiv 18 \pmod{20},$$

所以由中国剩余定理知

$$x = 13k - 6 \equiv 13 \times 18 - 6 \equiv 228 \pmod{260}.$$

在给定的某一年中，不能显然地说Oc 11在Etznab 5之前（我们必须检查）．如果确实如此，则它们之间有228天；否则它们之间有$32 = 260 - 228$天（事实是228天）． ◀ 71

→ **例 1.79（公钥密码）** 在A和B的一次战争中，A的间谍了解到B计划的一次突然袭击，所以他们一定要设法送一个紧急信息给自己的一方．若是B知道他们的计划被A知道了，他们当然会改变计划，所以A的间谍要在送出信息之前给信息加上密码．

把一份英文信息改成数字是没有任何问题的．把52个英文字母（小写和大写）和一个空格

⊖ 我们既可以拿1到19之间的数一个一个地试，也可以利用欧几里得算法来求出17．

以及 11 个间隔符

$$, \; . \; ; \; : \; ! \; ? \; - \; ' \; " \; (\;)$$

排成一列，总之一共是 64 个符号. 给每个符号分配一个二进制数. 例如，

$$\mathrm{a} \mapsto 01, \cdots, \mathrm{z} \mapsto 26, \mathrm{A} \mapsto 27, \cdots, \mathrm{Z} \mapsto 52$$

$$\text{space} \mapsto 53, . \mapsto 54, , \mapsto 55, \cdots, (\mapsto 63,) \mapsto 64.$$

一个密码是一个代码，在这个代码中原来信息中的不同字母被不同符号所取代. 解开任何密码都不是一件难事，实际上，许多报纸都会印一些日常的密码来娱乐读者. 在我们刚才所描述的密码中，"I love you"被编成密码为

$$\text{I love you.} = 3553121522055325152154.$$

注意，这个密码中的每个被编码的信息有偶数个数字，所以译码，即把数字变回英文是一件简单的事情. 因此，

$$\begin{aligned}3553121522055325152154 &= (35)(53)(12)(15)(22)(05)(53)(25)(15)(21)(54)\\ &= \text{I love you.}\end{aligned}$$

怎样编一个好的代码？若一个信息是一个自然数 x(这是不失一般性的)，我们需要一种方法将 x 编码(用一种很常规的方法，为了避免将错误传人被编码的信息中)，而且我们需要一种(很常规的)方法使接收信息的人译码这个信息. 最重要的是安全性：未被授权的人读到这个(被编码的)信息时不能将它译码. 一个有创意的方法是找到满足一些性质的密码，这些性质称为 RSA 公钥密码系统，是瑞斯特(R. Rivest)、沙米尔(A. Shamir)和艾德曼(L. Adleman)在 1978 年发现的，他们因这个发明而获得了 2002 年的图灵奖.

给定自然数 N，s 和 t，假设对每个自然数 x 有 $x^{st} \equiv x \pmod N$. 我们可将任意自然数 $x < N$ 编码为 $[x^s]_N$，即 x^s 模 N 的余数，若我们知道数 t，则可以译码，这是因为

$$(x^s)^t = x^{st} \equiv x \pmod N.$$

72 还要找出一个好密码所要满足的几个标准的数 N，s 和 t.

编码和译码的轻松

假设 N 有 d 个(十进位)数字. 只需展示怎样将一个最多含有 d 个数字的数编码，这是因为我们可以将一个更长的数分解成一些至多含有 d 个数字的块. 对 x^s 模 N 的计算基于这样一个事实：用电脑很容易计算 x^2 模 N. 因为计算 x^{2^i} 主要是计算 2 的 i 次幂，所以这也是容易的事情. 现在把指数 s 写成以 2 为底数的表示式，使得计算 x^s 就是计算一些 2 的幂：若 $m = 2^i + 2^j + \cdots + 2^z$，则 $x^m = x^{2^i + 2^j + \cdots + 2^z} = x^{2^i} x^{2^j} \cdots x^{2^z}$. 简言之，电脑用这种方法可以很容易地将一个信息编码.

译码需要计算 $(x^s)^t$ 模 N，如果我们像上面那样把 t(假设 t 已知)写成以 2 为底数的表示式，那么这也是一件很容易的事情.

构造 N 和 $m = st$

选取不同素数 p 和 q，它们都模 3 同余于 2，并定义 $N = pq$. 若 $m \geqslant p$，则由费马定理知

$$x^m = x^{m-p} x^p \equiv x^{m-p} x = x^{m-(p-1)} \pmod p.$$

若 $m - (p-1) \geqslant p$，我们可重复这个过程，直到得出

$$
\begin{aligned}
x^{m-(p-1)} &= x^{m-(p-1)-p}x^{p}\\
&\equiv x^{m-(p-1)-p}x\\
&= x^{m-2(p-1)}\\
&\ \ \vdots\\
&\equiv x^{m-h(p-1)}\pmod{p},
\end{aligned}
$$

其中 h 是满足 $m-h(p-1)\geqslant 0$ 的最大整数．但是这只是除法算式：$m=h(p-1)+r$，其中 r 是 m 被 $p-1$ 除后的余数．因而，对所有 x 有

$$x^{m}\equiv x^{r}\pmod{p}.$$

因此，若 $m\equiv 1(\mathrm{mod}(p-1))$，则对所有 x 有

$$x^{m}\equiv x\pmod{p}.$$

类似地，若 $m\equiv 1(\mathrm{mod}(q-1))$，则对所有 x 有 $x^{m}\equiv x(\mathrm{mod}\ q)$．因此，若 m 满足

$$m\equiv 1(\mathrm{mod}(p-1)(q-1)),$$

则 $m\equiv 1(\mathrm{mod}(p-1))$ 和 $m\equiv 1(\mathrm{mod}(q-1))$．因此，$x^{m}\equiv x(\mathrm{mod}\ p)$ 和 $x^{m}\equiv x(\mathrm{mod}\ q)$，即 $p\mid(x^{m}-x)$ 和 $q\mid(x^{m}-x)$．因为 p 和 q 是不同的素数，所以它们互素，所以由习题 1.60 知， 73
$pq\mid(x^{m}-x)$，即 $x^{m}\equiv x(\mathrm{mod}\ pq)$．因为 $N=pq$，所以我们已经证明了若 $m\equiv 1(\mathrm{mod}(p-1)(q-1))$，则对所有 x 有

$$x^{m}\equiv x\pmod{N}.$$

最后只需对给定的 p 和 q 求出数 $m\equiv 1(\mathrm{mod}(p-1)(q-1))$ 和分解式 $m=st$．我们断言存在一个分解式满足 $s=3$．我们先证明 $(3,(p-1)(q-1))=1$．因为 $p\equiv 2(\mathrm{mod}\ 3)$ 和 $q\equiv 2(\mathrm{mod}\ 3)$，所以 $p-1\equiv 1(\mathrm{mod}\ 3)$ 和 $q-1\equiv 1(\mathrm{mod}\ 3)$，因而 $(p-1)(q-1)\equiv 1(\mathrm{mod}\ 3)$，所以 3 和 $(p-1)(q-1)$ 互素(命题 1.34)．因此存在整数 t 和 u 满足 $1=3t+(p-1)(q-1)u$，所以 $3t\equiv 1(\mathrm{mod}(p-1)(q-1))$．总之，对 t 的这个选取，$x^{3t}\equiv x(\mathrm{mod}\ N)$ 对所有 x 成立．选取 $m=3t$ 则完成了这个密码要素的构造．

安全性

因为 $3t\equiv 1(\mathrm{mod}(p-1)(q-1))$，所以知道分解式 $N=pq$ 的人就会知道数 $(p-1)(q-1)$，因而就可以利用欧几里得算法求出 t．未被授权的读者可能知道 N，但是他若不知道分解式，则不会知道 t，因而不能译码．这就是这个密码安全的原因．例如，若 p 和 q 都有大约 200 位数字(且因为技术的原因，它们不会很接近)，则世上运算最快的计算机也需要两三个月的时间来分解 N．根据命题 1.62，存在很多素数模 3 同余于 2，所以我们可以每个月选取一对不同的素数 p 和 q，从而达到扰乱敌人的目的． ◀

习题

H 1.77 判断对错并说明理由．

(i)若 a，m 都是整数且 $m>0$，则存在某个整数 i 可使 $a\equiv i(\mathrm{mod}\ m)$，并且 $0\leqslant i\leqslant m-1$．

(ii)若 a，b，m 都是整数且 $m>0$，则由 $a\equiv b(\mathrm{mod}\ m)$ 可推出 $(a+b)^{m}\equiv a^{m}+b^{m}(\mathrm{mod}\ m)$．

(iii)若 a 是一个整数，则 $a^{6}\equiv a(\mathrm{mod}\ 6)$．

(iv)若 a 是一个整数，则 $a^{4}\equiv a(\mathrm{mod}\ 4)$．

(v)5263980007是一个完全平方数.

(vi)存在整数 n 满足 $n\equiv1(\mathrm{mod}\ 100)$ 和 $n\equiv4(\mathrm{mod}\ 1000)$.

(vii)存在整数 n 满足 $n\equiv1(\mathrm{mod}\ 100)$ 和 $n\equiv4(\mathrm{mod}\ 1001)$.

(viii)若 p 是素数且 $m\equiv n(\mathrm{mod}\ p)$，则对每个自然数 a 有 $a^m\equiv a^n(\mathrm{mod}\ p)$.

1.78 求出以下每个同余方程的所有整数解 x：

(i) $3x\equiv2(\mathrm{mod}\ 5)$.

74 (ii) $7x\equiv4(\mathrm{mod}\ 10)$.

(iii) $243x+17\equiv101(\mathrm{mod}\ 725)$.

(iv) $4x+3\equiv4(\mathrm{mod}\ 5)$.

(v) $6x+3\equiv4(\mathrm{mod}\ 10)$.

(vi) $6x+3\equiv1(\mathrm{mod}\ 10)$.

H 1.79 设 m 是一个正整数，并设 m' 是由重排 m 的(十进制)数字得到的整数(例如，取 $m=314\ 159$，$m'=539\ 114$). 证明 $m-m'$ 是9的倍数.

H 1.80 证明正整数 n 能被11整除当且仅当其各位数字的交错和能被11整除(若 a 的数字是 $d_k\cdots d_2d_1d_0$，则其交错和为 $d_0-d_1+d_2-\cdots$).

H 1.81 问7除 10^{100} 的余数是多少？(大数 10^{100} 在儿童故事中被称为googol⊖).

*1.82 (i)证明 $10q+r$ 被7整除当且仅当 $q-2r$ 被7整除.

(ii)给定整数 a，其十进制数字为 $d_kd_{k-1}\cdots d_0$，定义

$$a'=d_kd_{k-1}\cdots d_1-2d_0.$$

证明，a 被7整除当且仅当 a'，a''，a'''，…，中的某一个被7整除. (例如，若 $a=65\ 464$，则 $a'=6546-8=6538$，$a''=653-16=637$，$a'''=63-14=49$，由此得65 464被7整除.)

*1.83 (i)证明 $1000\equiv-1(\mathrm{mod}\ 7)$.

(ii)证明：若 $a=r_0+1000r_1+1000^2r_2+\cdots$，则 a 被7整除当且仅当 $r_0-r_1+r_2-\cdots$ 被7整除.

注：习题1.82和1.83一起给出了确定大数是否被7整除的有效方法. 例如，若 $a=33\ 456\ 789\ 123\ 987$，则 $a\equiv0(\mathrm{mod}\ 7)$ 当且仅当 $987-123+789-456+33=1230\equiv0(\mathrm{mod}\ 7)$. 根据习题1.82，$1230\equiv123\equiv6(\mathrm{mod}\ 7)$，所以 a 不被7整除.

*1.84 给定正整数 m，求出满足 $0<r<m$ 且使得 $2r\equiv0(\mathrm{mod}\ m)$ 的所有整数 r.

H 1.85 证明满足 $x^2+y^2+z^2=999$ 的整数 x，y，z 不存在.

H 1.86 证明末位两个数字是35的完全平方数 a^2 不存在.

1.87 设 x 是不被3整除的奇数，证明 $x^2\equiv1(\mathrm{mod}\ 24)$.

*H 1.88 证明：若 p 是素数且 $a^2\equiv1(\mathrm{mod}\ p)$，则 $a\equiv\pm1(\mathrm{mod}\ p)$.

*1.89 考虑同余方程 $ax\equiv b(\mathrm{mod}\ m)$，其中 $\gcd(a,m)=d$. 证明 $ax\equiv b(\mathrm{mod}\ m)$ 有解当且仅当 $d\mid b$.

H 1.90 解同余方程 $x^2\equiv1(\mathrm{mod}\ 21)$.

1.91 解同余方程组：

(i) $x\equiv2(\mathrm{mod}\ 5)$，$3x\equiv1(\mathrm{mod}\ 8)$；

(ii) $3x\equiv2(\mathrm{mod}\ 5)$，$2x\equiv1(\mathrm{mod}\ 3)$.

75 H 1.92 求被5，7，9除后余数分别为4，3，1的最小正整数.

⊖ 这个词是由一个9岁男孩发明的，当时他的叔叔要他给1后面有100个零的数取一个名字. 同时这个男孩还建议给1后面有googol个零的数取名为googolplex.

1.93　在玛雅人的卓尔金历中，Akbal 13 和 Muluc 8 之间相隔多少天？

1.94　H (i)证明，对所有整数 a，b 和 $n\geqslant 1$ 有 $(a+b)^n\equiv a^n+b^n \pmod 2$．

(ii)证明 $(a+b)^2\not\equiv a^2+b^2 \pmod 3$．

1.95　解线性系统

$$x\equiv 12 \pmod{25}$$
$$x\equiv 2 \pmod{30}.$$

*1.96　设 m，m' 都是正整数，$d=(m, m')$，$b\equiv b' \pmod d$．证明系统

$$x\equiv b \pmod m$$
$$x\equiv b' \pmod{m'}.$$

的任意两个解都模 ℓ 同余，其中 $\ell=\operatorname{lcm}\{m, m'\}$．

H 1.97　在一个荒岛上，有五个人和一只猴子，他们白天采集完椰子，然后睡觉．第一个人醒了，决定取走自己的那份椰子．他把椰子等分成五份，还多出一个，他把多出的这个椰子给了猴子，把自己的那份藏好后，继续睡觉．过了一会儿，第二个人醒了，他取走剩下的这堆椰子的五分之一，也发现多出一个，他也把这个多出的椰子给了猴子．其他三个人也依次做了与前面两人类似的事情．请找出一开始的这堆椰子的最小数目．

→1.6　日期与天数

同余可用来确定给定的某一天是星期几．例如，1776 年 7 月 4 日是星期几？

一年是指地球绕太阳旋转一周所花的时间．**一天**是指地球绕穿过南北两极的地轴旋转一周所花的时间．要求一年中的天数是一个整数，这是没有道理的，它也确实不是．一年大约是 365.2422 天这么长．公元前 46 年，罗马的凯撒大帝（和他的科学顾问）通过创立**儒略历法**(Julian calendar)来弥补这一点．在儒略历法中，每四年有一个**闰年**，即每四年多一天，即 2 月 29 日，这一年有 366 天（非闰年的年份称为**平年**）．若一年恰有 365.25 天，这样做虽然是很好的，但实际上使一年长了 365.25－365.2422＝0.0078 天（约为 11 分 14 秒）．128 年之后，日历中要加上一天．在 1582 年，春分（春天里白天和黑夜各为 12 小时的那一天）是 3 月 11 日，而不是 3 月 21 日．教皇葛里高利十三世（和他的科学顾问）在 1582 年建立了**葛里高利历法**(Gregorian calendar)，抹去了 10 天．1582 年 10 月 4 日的后一天是 1582 年 10 月 15 日，这引起了人们的困惑和害怕．葛里高利历法是按如下方法修改儒略历法的：以 00 结尾的年份称为 76
世纪年．当 y 年不是世纪年时，若 y 能被 4 整除则 y 年是闰年；当 y 年是世纪年时，仅当 y 能被 400 整除时 y 年才是闰年．例如，1900 年不是闰年，而 2000 年是闰年．葛里高利历法是今天通用的历法，但不是整个欧洲唯一采用的历法．例如，英国直到 1752 年才采用它，那年抹去了 11 天；俄国直到 1918 年才采用，抹去了 13 天（因此俄国称他们的 1917 年革命为十月革命，尽管按葛里高利历法计算革命发生在11 月）．

400 年的实际天数大约是

$$400\times 365.2422=146\,096.88 \text{ 天}$$

按儒略历法，400 年有

$$400\times 365+100=146\,100 \text{ 天}$$

而按葛里高利历法，400 年有 146 097 天（这一时期删去了 3 个闰年）．因此，儒略历法每 400

年多出 3.12 天，而葛里高利历法每 400 年仅多出 0.12 天(大约 2 小时 53 分).

稍微计算一下就知道公元前 46 年到 1582 年之间有 1628 年．儒略历法每 128 年多出 1 天，因此 1628 年中多出了 13 天(因为 $13\times128=1662$)．为什么葛里高利没有抹去这 13 天呢？在 325 年的尼西亚会议(Council of Nicaea)上，复活节被定为圆月后的第一个星期天，因为这是在春分那天或春分之后的第一个圆月之日．325 年的春分是 3 月 21 日，664 年才正式把春分定为 3 月 21 日．1582 年所观察到的结果与按儒略历法算出的 $1257=1582-325$ 年的结果相差大约 10 天.

现在寻找一个历法公式．尽管不存在为零的年份，但为了容易计算，我们选 0000 为参考年！给一个星期的每一天分配一个数，按下面方法分配：

星期日	星期一	星期二	星期三	星期四	星期五	星期六
0	1	2	3	4	5	6

特别，0000 年 3 月 1 日对应 a，$0\leqslant a\leqslant 6$．则 0001 年 3 月 1 日对应 $a+1 \pmod 7$，这是因为从 0000 年 3 月 1 日到 0001 年 3 月 1 日历经了 365 天，且

$$365=52\times7+1\equiv1 \pmod 7).$$

类似地，0002 年 3 月 1 日对应 $a+2$，0003 年 3 月 1 日对应 $a+3$．但是 0004 年 3 月 1 日对应 $a+5$，这是因为在 0003 年 3 月 1 日与 0004 年 3 月 1 日之间有 0004 年 2 月 29 日，所以从前一

77 个 3 月 1 日以来，过去了 $366\equiv2 \pmod 7$ 天．因此我们看到，每个平年 3 月 1 日对应的数是在前一年这一天对应的数上加 1，而每个闰年 3 月 1 日对应的数是在前一年 3 月 1 日对应的数上加 2．因此，若 0000 年 3 月 1 日对应 a，则 y 年 3 月 1 日对应的数 a' 为

$$a'\equiv a+y+L \pmod 7,$$

其中 L 是从 0000 年到 y 年之间闰年的数目．为计算 L，计算能被 4 整除的那些年有多少，然后去掉所有世纪年，再把是闰年的世纪年加回来．因此

$$L=\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor,$$

其中 $\lfloor x\rfloor$ 表示不大于 x 的最大整数．因此，我们有

$$\begin{aligned} a' &\equiv a+y+L \\ &\equiv a+y+\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor \pmod 7 \end{aligned}$$

实际上我们可以通过看日历找到 a' 的值．因为 1994 年 3 月 1 日是星期二，所以

$$\begin{aligned} 2 &\equiv a+1994+\lfloor 1994/4\rfloor-\lfloor 1994/100\rfloor+\lfloor 1994/400\rfloor \\ &\equiv a+1994+498-19+4 \pmod 7, \end{aligned}$$

所以

$$a\equiv-2475\equiv-4\equiv3 \pmod 7$$

(即 0000 年 3 月 1 日是星期三)．我们现在可以确定任何一年 $y>0$ 的 3 月 1 日是星期几，即这一天对应

$$3+y+\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor \pmod 7.$$

我们之所以讨论 3 月 1 日是有原因的．假使罗马的凯撒大帝下令：闰年中多余一天是 12

月 32 日，而不是 2 月 29 日，那么生活会更简单.⊖让我们来分析一下 2 月 28 日. 例如，假设 1600 年 2 月 28 日对应 b. 因为 1600 年是闰年，所以 1600 年 2 月 29 日在 1600 年 2 月 28 日与 1601 年 2 月 28 日之间，因而在两个 2 月 28 日之间历经了 366 天，所以 1601 年 2 月 28 日对应 78
$b+2$，1602 年 2 月 28 日对应 $b+3$，1603 年 2 月 28 日对应 $b+4$，1604 年 2 月 28 日对应 $b+5$，但 1605 年 2 月 28 日对应 $b+7$(因为 1604 年有 2 月 29 日).

让我们对 1600 年 2 月 28 日与 1599 年某一天的变化方式做个比较. 1600 年 2 月 28 日的变化方式为 b，$b+2$，$b+3$，$b+4$，$b+5$，$b+7$，…. 若 1599 年 5 月 26 日对应 c，则 1600 年 5 月 26 日对应 $c+2$，这是因为两个 5 月 26 日之间有 1600 年 2 月 29 日，因而其间有 $366\equiv 2(\mathrm{mod}\ 7)$天. 以后的几个 5 月 26 日，从 1601 年 5 月 26 日开始，分别对应 $c+3$，$c+4$，$c+5$，$c+7$. 我们看到，从 1600 年开始的 2 月 28 日的变化方式与从 1599 年开始的 5 月 26 日的变化方式完全相同. 因此，y 年的 1 月或 2 月中任何一天的变化方式与 $y-1$ 年中任何一天的变化方式是相同的：闰年的前一年要在日期的对应数上加 2，而所有其他年都只要加 1. 因此，我们恢复新年这一天落在 3 月 1 日的古历，1 月或 2 月里的任何一天被看作属于前一年.

我们怎么确定非 3 月 1 日的任何一天是星期几呢？由于 0000 年 3 月 1 日对应 3(正如我们在上面所看到的)，所以 0000 年 4 月 1 日对应 6，这是因为 3 月有 31 天，且 $3+31\equiv 6(\mathrm{mod}\ 7)$. 因为 4 月有 30 天，所以 0000 年 5 月 1 日对应 $6+30\equiv 1(\mathrm{mod}\ 7)$. 这里有一个表，给出了 0000 年每个月的第一天对应的数(见表 1-2)：

表 1-2　每月的第一天

日期	数字	日期	数字	日期	数字
3 月 1 日	3	7 月 1 日	6	11 月 1 日	3
4 月 1 日	6	8 月 1 日	2	12 月 1 日	5
5 月 1 日	1	9 月 1 日	5	1 月 1 日	1
6 月 1 日	4	10 月 1 日	0	2 月 1 日	4

记住，我们是假设 3 月为 1 月，4 月为 2 月，等等. 记上面这些数为 $1+j(m)$，对 $m=1, 2, \cdots, 12$，定义 $j(m)$为

$$j(m): 2,5,0,3,5,1,4,6,2,4,0,3.$$

于是 y 年 m 月 1 日对应

$$1+j(m)+g(y)(\mathrm{mod}\ 7),$$

其中

$$g(y)=y+\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor.$$ 79

⊖ 实际上，在古罗马历中 3 月 1 日是一年中的第一天. 这解释了为什么闰年多出的这一天被加到 2 月而不是其他月份. 它还解释了为什么第 9，10，11 和 12 月分别取名为 September，October，November，December. 在开始时，它们分别是第 7，8，9 和 10 月.

按葛里高利历法，乔治・华盛顿应出生于 1732 年 2 月 22 日. 但是直到 1752 年葛里高利历法才传入英国的殖民地. 这样他的原始生日是 2 月 11 日. 因为新年由 3 月 1 日变为 1 月 1 日，所以 1731 年中的 2 月应当被看作 1732 年中的月份. 乔治・华盛顿曾经开玩笑说：不仅他的生日改变了，而且他的出生年份也改变了. 见习题 1.102.

命题 1.80 (日历[⊖]公式) 假设1月和2月里的日期被当作前一年的日期，则 y 年 m 月 d 日对应的数为

$$d+j(m)+g(y)(\mathrm{mod}\ 7),$$

其中

$$j(m)=2,5,0,3,5,1,4,6,2,4,0,3$$

(3月对应 $m=1$，4月对应 $m=2$，…，2月对应 $m=12$)且

$$g(y)=y+\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor.$$

证明 y 年 m 月1日对应的数为 $1+j(m)+g(y)(\mathrm{mod}\ 7)$，于是 y 年 m 月2日对应 $2+j(m)+g(y)$，一般地，y 年 m 月 d 日对应 $d+j(m)+g(y)$. ■

例 1.81 利用日历公式求出1776年7月4日是星期几？这里 $m=5$，$d=4$，$y=1776$. 代入公式得

$$4+5+1776+444-17+4=2216\equiv 4(\mathrm{mod}\ 7);$$

因此，1776年7月4日是星期四. ◀

大多数人利用日历公式计算时需要用纸和笔(或计算器). 这里有几种方法可以简化公式，使人们只要在头脑中做计算，并且可以让自己的朋友惊讶一下.

$j(m)$的记忆方法之一如下：

$$j(m)=\lfloor 2.6m-0.2\rfloor,\quad 1\leqslant m\leqslant 12.$$

$j(m)$的另一个记忆方法是下述句子：

My	Uncle	Charles	has	eaten	a	cold	supper;	he	eats	nothing	hot.
2	5	(7≡0)	3	5	1	4	6	2	4	(7≡0)	3

推论 1.82 假设1月和2月里的日期被视为是前一年的，则 $y=100C+N$ 年 m 月 d 日，其中 $0\leqslant N\leqslant 99$，对应

80

$$d+j(m)+N+\lfloor N/4\rfloor+\lfloor C/4\rfloor-2C(\mathrm{mod}\ 7).$$

证明 若记 $y=100C+N$，$0\leqslant N\leqslant 99$，则

$$y=100C+N\equiv 2C+N(\mathrm{mod}\ 7).$$
$$\lfloor y/4\rfloor=25C+\lfloor N/4\rfloor\equiv 4C+\lfloor N/4\rfloor(\mathrm{mod}\ 7),$$
$$\lfloor y/100\rfloor=C,\quad \lfloor y/400\rfloor=\lfloor C/4\rfloor.$$

因此，

$$\begin{aligned}y+\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor&\equiv N+5C+\lfloor N/4\rfloor+\lfloor C/4\rfloor(\mathrm{mod}\ 7)\\&\equiv N+\lfloor N/4\rfloor+\lfloor C/4\rfloor-2C(\mathrm{mod}\ 7).\end{aligned}$$ ■

这个公式比第一个更简单. 例如，1776年7月4日的对应数为

$$4+5+76+19+4-34=74\equiv 4(\mathrm{mod}\ 7),$$

与例1.81中的计算相符合. 读者现在可以知道他或她的出生日期是星期几.

例 1.83 丹尼和埃拉的祖母安娜的出生日期都是1906年12月5日，那么她是星期几出生

⊖ “日历(calendar)”来自希腊文“to call”，后来演变成拉丁文，意指一个月的第一天(账目预期到达的时间).

的呢?

设 A 是这一天对应的数，则

$$\begin{aligned}A &\equiv 5+4+6+\lfloor 6/4\rfloor+\lfloor 19/4\rfloor-38\\ &\equiv -18 \pmod 7\\ &\equiv 3 \pmod 7).\end{aligned}$$

安娜出生在星期三. ◀

每个 y 年都有一个星期五对应 13 吗？我们有

$$5\equiv 13+j(m)+g(y) \pmod 7.$$

若当 m 从 1 变到 12 时，$j(m)$ 取遍 0 到 6(mod 7)，则回答是肯定的. 对模 7 的余数序列是

$$2,5,\boxed{0},\boxed{3},\boxed{5},\boxed{1},\boxed{4},\boxed{6},\boxed{2},4,0,3.$$

事实上，我们看到，5 月与 11 月之间一定有一个星期五对应 13. 上列数中没有哪个出现过 3 次，但是可能一年中存在三个星期五对应 13，这是因为 1 月和 2 月被视为前一年的月份. 例如，1987 年有三个星期五对应 13(见习题 1.101). 当然，我们可以用其他星期几取代星期五，也可以用 1 与 28 之间的任何数代替 13 来讨论. 81

康威(J. H. Conway)找到了一个更简单的日历公式. 在他的体系中，称一年中的**审判日**为 2 月的最后一天所在的星期几(如表 1-3). 例如，1900 年的审判日对应于 1900 年 2 月 28 日(1900 年不是闰年)，是星期三=3，而 2000 年的审判日对应于 2000 年 2 月 29 日，是星期二=2，这些正如我们利用推论 1.82 所计算的一样.

表 1-3 审判日

1600 年 2 月 29 日	2	星期二
1700 年 2 月 28 日	0	星期日
1800 年 2 月 28 日	5	星期五
1900 年 2 月 28 日	3	星期三
2000 年 2 月 29 日	2	星期二

知道了世纪年 $100C$ 年的审判日后，我们便可以找出这个世纪里任何其他年份 $y=100C+N$ 的审判日. 方法如下：因为 $100C$ 年是世纪年，所以从 $100C$ 年到 y 年，闰年的数目不包含葛里高利历法变更. 因此，若 D 是 $100C$ 年的审判日(当然 $0\leqslant D\leqslant 6$)，则 $100C+N$ 年的审判日同余于

$$D+N+\lfloor N/4\rfloor \pmod 7.$$

例如，因为 1900 年的审判日是星期三=3，可知 1994 年的审判日是星期一=1，这是因为

$$3+94+23=120\equiv 1 \pmod 7.$$

命题 1.84 (康威公式) *设 D 是 $100C$ 年的审判日，并设 $0\leqslant N\leqslant 99$. 若 $N=12q+r$，$0\leqslant r<12$，则 $100C+N$ 年的审判日的计算公式是*

$$D+q+r+\lfloor r/4\rfloor \pmod 7.$$

证明

$$\begin{aligned}100C+N\text{ 年的审判日} &\equiv D+N+\lfloor N/4\rfloor\\ &\equiv D+12q+r+\lfloor (12q+r)/4\rfloor\\ &\equiv D+15q+r+\lfloor r/4\rfloor\\ &\equiv D+q+r+\lfloor r/4\rfloor \pmod 7.\end{aligned}$$

■

例如，$94=12\times 7+10$，所以 1994 年的审判日是 $3+7+10+2\equiv 1 \pmod 7$，即 1994 年的审判日是星期一，这正如上面所看到的一样. 82

如果我们知道了某个特殊年份的审判日是星期几，那就可以利用各种技巧(例如，my Uncle Charles)把这一年的审判日变为这一年的其他任何一天. 康威观察到，有一些日期与审判日是在一周的同一天，它们是

4 月 4 日，　6 月 6 日，　8 月 8 日，　10 月 10 日，　12 月 12 日，

5 月 9 日，　7 月 11 日，　9 月 5 日，　11 月 7 日.

若回到以 1 月为第一个月的常用计法上来：1=1 月，则使用下述记号会更容易记住这些日期：

4/4,6/6,8/8,10/10,12/12,5/9,7/11,9/5,11/7,

其中 m/d 表示月/日. 由于审判日对应于 2 月的最后一天，所以我们处在日历中任何日期的几个星期内，并能很容易地找到想要的那一天.

习题

H 1.98　一个嫌疑犯说 1893 年 4 月 21 日他和他生病的母亲在一起过复活节，私人侦探夏洛克·福尔摩斯认为他说了假话. 那么这位著名侦探是怎样肯定嫌疑犯说了假话呢?

H 1.99　在 1900 年有多少个月的第一天是星期二?

H 1.100　1896 年 2 月 29 日是星期几? 从你的解决方法中可知：判断闰年的那一天是星期几也不难.

*1.101　(i)证明 1987 年有三个星期五对应 13.

(ii)证明：对任意年份 $y>0$，有 $g(y)-g(y-1)=1$ 或 2，这里 $g(y)=y+\lfloor y/4\rfloor-\lfloor y/100\rfloor+\lfloor y/400\rfloor$.

H (iii)是否有某一年只有一个星期五对应 13?

H 1.102　我叔叔说他出生于 1900 年 2 月 29 日，我告诉他这不可能，因为 1900 年不是闰年. 为什么我是错误的?

83

第2章 群 I

群论是伽罗瓦(E. Galois，1811—1832)为了解决他那个时代的几个首要的数学问题之一而创造的，那个问题是：什么时候可以用二次公式的某个推广来找到一个多项式的根？自伽罗瓦(他在一次决斗中去世，年仅 20 岁)以来，群论已经建立了许多其他的应用．例如，我们将给出费马定理(若 p 是素数，则 $a^p \equiv a \bmod p$)的一个新的证明，且这个证明适合于证明欧拉的一个定理：若 $m \geqslant 2$，则 $a^{\phi(m)} \equiv 1 \bmod m$，其中 $\phi(m)$是欧拉 ϕ-函数．我们也将利用群解决如下的计数问题：多少个有 10 颗珠子的不同手镯可以聚集成含有 10 个红珠子，10 个白珠子和 10 个蓝珠子的一堆？在第 6 章我们会阐述一个事实：群通过对平面中的所有椭进行分类来恰当地描述对称性．

→2.1 一些集合理论

一个群是一个集合，其元素可以被"乘"，且乘法遵从一定的法则．群的重要例子是其元素为置换且置换是某些函数．另外，我们用函数将两个群作比较，称为同态．因此这一部分包含了一些定义以及函数的基本性质．若读者以前看过这部分内容，则此处可以跳过，以后有需要时再回头来看．

集合 X 是指某些特定事物(数，点，青鱼等等)组成的一个整体，组成这个整体的事物叫做集合的元素．若 x 是集合 X 的一个元素，就说 x 属于 X，记作 $x \in X$.[⊖]两个集合 X 和 Y 是 84
相等的，记作

$$X = Y,$$

如果它们由完全相同的元素组成，即对任何元素 x，都有 $x \in X$ 当且仅当 $x \in Y$.

集合 S 称为集合 X 的**子集**，是指 S 的所有元素都属于 X，即若 $s \in S$ 则 $s \in X$．我们用

$$S \subseteq X$$

表示 S 是 X 的子集．S 是 X 的子集，也叫做 S **包含于** X．$X \subseteq X$ 总是成立的．X 的子集 S 叫做 X 的**真子集**，记为 $S \subsetneq X$，如果 $S \subseteq X$ 且 $S \neq X$．两个集合 X 与 Y 是相等的当且仅当每个集合是另一个集合的子集：

$$X = Y \quad \text{当且仅当} \quad X \subseteq Y \text{ 且 } Y \subseteq X.$$

根据这一点，我们在证明两个集合相等时，往往需要证明两部分，每部分都证明一个集合是另一个的子集．例如，令

$$X = \{a \in \mathbb{R} : a \geqslant 0\}, \quad Y = \{b \in \mathbb{R} : b = r^2, r \in \mathbf{R}\}.$$

设 $a \in X$，则 $a \geqslant 0$，且 $a = r^2$，其中 $r = \sqrt{a}$，因此 $a \in Y$，这样 $X \subseteq Y$．对于反包含，取 $b \in Y$，使得对某个 $r \in \mathbb{R}$ 有 $b = r^2 \in Y$．当 $r \geqslant 0$ 时，$r^2 \geqslant 0$；当 $r < 0$ 时，令 $r = -s(s > 0)$，则 $r^2 = (-1)^2 s^2 = s^2 \geqslant 0$．总之 $b = r^2 \geqslant 0$ 且 $b \in X$．因此 $Y \subseteq X$．所以 $X = Y$.

→ **定义** **空集**是指不含任何元素的集合$\varnothing$.

⊖ $\in$ 的使用是有规则的．例如，$x \in a \in x$ 总是一个假命题．

我们断言，对每个集合 X 有 $\varnothing\subseteq X$. “若 $s\in\varnothing$ 则 $s\in X$”的否命题是“存在 $s\in\varnothing$ 使 $s\notin X$”. 但是，因为不存在 $s\in\varnothing$，所以这个命题不可能成立. 于是空集是唯一存在的，因为若 $\varnothing_1$ 是另一个空集，则 $\varnothing\subseteq\varnothing_1$，同样有 $\varnothing_1\subseteq\varnothing$，因此 $\varnothing=\varnothing_1$.

以下给出了从一些集合中构造出新的集合的方法，见图 2-1.

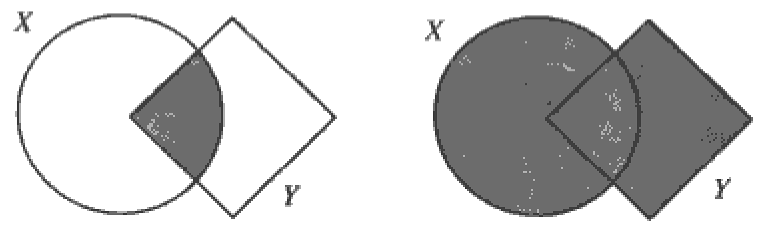


图 2-1 $X\cap Y$ 和 $X\cup Y$

定义 若 X，Y 都是 Z 的子集，则它们的**交**是集合

$$X\cap Y=\{z\in Z: z\in X \text{ 且 } z\in Y\}.$$

更一般地，若 $\{A_i: i\in I\}$ 是集合 Z 的任意一族子集，可能无穷多个，则它们的**交**是

85 $$\bigcap_{i\in I}A_i=\{z\in Z: z\in A_i \text{ 对所有 } i\in I \text{ 成立}\}.$$

显然有 $X\cap Y\subseteq X$，$X\cap Y\subseteq Y$. 事实上，交集是满足这样条件的最大集合：若 $S\subseteq X$ 且 $S\subseteq Y$，则 $S\subseteq X\cap Y$. 同样，$\bigcap_{i\in I}A_i\subseteq A_j$ 对所有 $j\in I$ 成立.

定义 若 X，Y 都是 Z 的子集，则它们的**并**是集合

$$X\cup Y=\{z\in Z: z\in X \text{ 或 } z\in Y\}.$$

更一般地，若 $\{A_i: i\in I\}$ 是集合 Z 的任意一族子集，可能无穷多个，则它们的**并**是

$$\bigcup_{i\in I}A_i=\{z\in Z: z\in A_i \text{ 对某个 } i\in I \text{ 成立}\}.$$

显然有 $X\subseteq X\cup Y$，$Y\subseteq X\cup Y$. 事实上，并集是满足这样条件的最小集合：若 $X\subseteq S$ 且 $Y\subseteq S$，则 $X\cup Y\subseteq S$. 同样，$A_j\subseteq\bigcup_{i\in I}A_i$ 对所有 $j\in I$ 成立.

定义 若 X，Y 都是集合，则它们的**差**是集合

$$X-Y=\{x\in X: x\notin Y\}.$$

差 $Y-X$ 有类似的定义. 当然，$Y-X$ 和 $X-Y$ 没有公共元素：$(Y-X)\cap(X-Y)=\varnothing$（见图 2-2 和图 2-3).

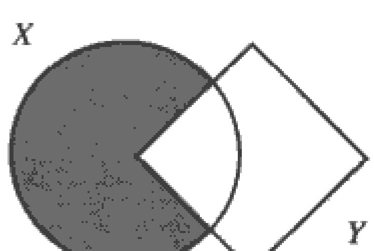


图 2-2 $X-Y$

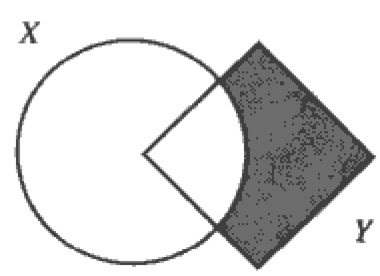


图 2-3 $Y-X$

特别地，若 X 是集合 Z 的一个子集，则它在 Z 中的补是集合

$$X' = Z - X = \{z \in Z : z \notin X\}.$$

显然，X'与 X **不相交**，即不存在元素 $z\in Z$ 既属于 X 又属于 X'，所以 $X\cap X'=\varnothing$.（因此，空集保证了两个子集 A 和 B 的交总是一个子集，即 $A\cap B$ 总是有定义.）事实上，X'是 Z 的与 X 不相交的最大子集：若 $S\subseteq Z$ 且 $S\cap X=\varnothing$，则 $S\subseteq X'$. 86

→2.1.1 函数

函数的思想出现在微积分中（甚至更早），例如 x^2，$\sin x$，$\sqrt{x}$，$1/x$，$x+1$，e^x 等都是函数. 微积分的书籍定义函数 $f(x)$为一个"法则"，该"法则"要求：对于每个数 a，恰好分配一个数即 $f(a)$与之对应. 因此，平方函数分配 81 给 9；平方根函数分配 3 给 9. 注意$\sqrt{9}$可能等于 3 或－3. 为了只分配一个数给 9，我们必须从两个可能值±3 中挑选一个，人们都认同只要 $x\geqslant 0$ 就有$\sqrt{x}\geqslant 0$，所以$\sqrt{x}$是一个函数.

函数的微积分定义当然是对的，但也有缺陷：法则是什么？用另一种方式问这个问题，什么时候两个法则相同？例如，考虑函数

$$f(x) = (x+1)^2 \quad 和 \quad g(x) = x^2+2x+1.$$

$f(x)=g(x)$成立吗？计算过程当然不同：例如，$f(6)=(6+1)^2=7^2$ 而 $g(6)=6^2+2\cdot 6+1=36+12+1$. 由于术语"法则"没有被定义，所以其含义是模糊的，我们的问题也就不能够回答. 如果我们不能确定两个函数是否相等，那么微积分对函数的描述显然是不充分的.

为了找到一个合理的定义，让我们回到寻求函数定义的例子上来. 函数 x^2，$\sin x$ 等中的每一个都有一个由形如$(a, f(a))$的点构成的图形，它是平面的子集. 例如，$f(x)=x^2$ 的图形是由所有形如(a, a^2)的点构成的抛物线.

图形是直观的东西，即将给出的函数的正式定义相当于描述函数具有自己的图形. 把函数当作法则的这个非正式微积分定义仍然保留，但是我们将避开什么是法则这个问题. 为给出定义，我们先要给出类似平面的概念（因为我们想利用函数 $f(x)$的自变量 x 是数值这个特性）. 87

→ **定义** 若 X，Y 都是集合（不一定不相同），则称所有有序对(x, y)构成的集合 $X\times Y$ 为它们的**笛卡儿积**[⊖]，其中 $x\in X$，$y\in Y$.

平面是$\mathbb{R}\times\mathbb{R}$.

关于有序对我们只需知道的是

$$(x,y) = (x',y') \quad 当且仅当 \quad x = x', y = y'$$

（见习题 2.5）.

若 X，Y 都是有限集，不妨设 $|X|=m$，$|Y|=n$（$|X|$ 表示有限集 X 的元素个数），则 $|X\times Y|=mn$.

→ **定义** 设 X，Y 都是集合（不一定不相同），子集 $f\subseteq X\times Y$. 若对每个 $a\in X$，存在唯一的 $b\in Y$ 使$(a, b)\in f$，则称 f 为 X 到 Y 的一个**函数**，记为

$$f : X \to Y.$$

对每个 $a\in X$，称满足$(a, b)\in f$ 的唯一元素 $b\in Y$ 为 f 在 a 处的**值**，并记 b 为 $f(a)$. 因

⊖ 这个术语是纪念笛卡儿（R. Descartes）的，他是解析几何创始人之一.

此，f 是由 $X\times Y$ 中所有形如$(a, f(a))$的点构成的. 当 $f: \mathbb{R}\to\mathbb{R}$ 时，f 是 $f(x)$的图像.

例 2.1 (i)设 X 是一个集合，则集合 X 上的**恒等函数**，记为 $1_X: X\to X$，定义为对每个 $x\in X$ 有 $1_X(x)=x$[当 $X=\mathbb{R}$ 时，恒等函数的图像是所有形如(a, a)的点构成的 45°直线].

(ii)**常数函数**：若 $y_0\in Y$，则对所有 $x\in X$ 有 $f(x)=y_0$(当 $X=\mathbb{R}=Y$ 时，常数函数的图像是水平直线). ◀

从现在开始，我们抛开微积分符号，用 f 表示一个函数，而不用 $f(x)$，当要表示 f 在元素 x 处的值时才用 $f(x)$(有一些例外的情况，我们将继续按通常的记号表示一些熟悉的函数，如多项式，$\sin x$，e^x，$\sqrt{x}$，$\log x$). 若 $f: X\to Y$，则称 X 为 f 的**定义域**，称 Y 为 f 的**目标域**(或上域)，并定义 f 的**象**(或范围)，记为 $\operatorname{im} f$，它是由所有 f 的值构成的 Y 的子集. 当我们说 X 是函数 $f: X\to Y$ 的定义域时，意思是 $f(x)$对每个 $x\in X$ 有定义. 例如，$\sin x$ 的定义域是 $\mathbb{R}$，目标域通常为 $\mathbb{R}$，象是$[-1, 1]$. $1/x$ 的定义域是所有非零实数构成的集合，其象也是非零实数集合. 平方根函数的定义域是所有非负实数构成的集合 $\mathbb{R}^{\geqslant}=\{x\in\mathbb{R}: x\geqslant 0\}$，其象也
88 是 $\mathbb{R}^{\geqslant}$.

定义 称两个函数 $f: X\to Y$，$g: X'\to Y'$ **相等**，若 $X=X'$，$Y=Y'$，且子集 $f\subseteq X\times Y$ 和 $g\subseteq X'\times Y'$ 相等.

函数 $f: X\to Y$ 有三个组成部分：定义域 X，目标域 Y 和图像. 我们说两个函数相等当且仅当它们有相同的定义域，相同的目标域和相同的图像. 显然，定义域和图像是一个函数的本质部分，在本节末尾的注中将给出关心目标域的一些原因.

定义 若 $f: X\to Y$ 是一个函数，S 是 X 的一个子集，则 f 对 S 的**限制**是函数 $f\mid S: S\to Y$，定义为对所有 $s\in S$ 有$(f\mid S)(s)=f(s)$.

若 S 是 X 的一个子集，则定义**包含** $i: S\to X$ 为如下函数：对所有 $s\in S$ 有 $i(s)=s$.

若 S 是 X 的一个真子集，则包含 i 不是恒等函数 1_S，因为它的目标域是 X 而不是 S；它也不是恒等函数 1_X，因为它的定义域是 S 而不是 X. 若 S 是 X 的一个真子集，则 $f\mid S\neq f$，因为它们的定义域不同.

命题 2.2 设 $f: X\to Y$，$g: X'\to Y'$ 都是函数. 则 $f=g$ 当且仅当 $X=X'$，$Y=Y'$，且对每个 $a\in X$ 有 $f(a)=g(a)$.

注 这个命题解决了由模糊术语"法则"产生的问题. 若 $f, g: \mathbb{R}\to\mathbb{R}$ 由 $f(x)=(x+1)^2$，$g(x)=x^2+2x+1$ 给定，则 $f=g$，因为对每个数 a 有 $f(a)=g(a)$.

证明 假设 $f=g$. 因为函数是 $X\times Y$ 的子集，所以 $f=g$ 的意思是 f 和 g 中的每一个都是另一个的子集(在非正式场合，我们说 f 和 g 有相同的图像). 若 $a\in X$ 且$(a, f(a))\in f=g$，则$(a, f(a))\in g$. 但是 g 中只有一个有序对的第一个坐标是 a，即$(a, g(a))$[因为函数的定义是说 g 对 a 给出唯一的一个值]. 因此，$(a, f(a))=(a, g(a))$，且由有序对的相等知 $f(a)=g(a)$，这正是我们所要证明的.

反之，假设对每个 $a\in X$ 有 $f(a)=g(a)$. 为证明 $f=g$，只需证明 $f\subseteq g$ 和 $g\subseteq f$. f 的每个元素有形式$(a, f(a))$. 由于 $f(a)=g(a)$，所以有$(a, f(a))=(a, g(a))$，因而$(a, f(a))\in g$. 因此 $f\subseteq g$. 相反的包含关系 $g\subseteq f$ 可类似证得. ■

让我们把反证法弄明确些：若函数 f，$g: X \to Y$ 取不同的值，甚至只在一点处取不同的值，即存在某个 $a \in X$ 使得 $f(a) \neq g(a)$，则 $f \neq g$.

我们继续把函数看作是把 $x \in X$ 映到 $f(x) \in Y$ 的一个法则，但是只要我们需要，就可以用精确的定义，如在命题 2.2 中一样．然而，为了强调函数 $f: X \to Y$ 把 X 中的点映到 Y 中的点这一动态行为，我们通常写

$$f: x \mapsto y$$ 89

而不写 $f(x)=y$．例如，我们可写 $f: x \mapsto x^2$，而不写 $f(x)=x^2$；可用 $f: x \mapsto x$ 描述恒等映射.

例 2.3 我们的定义允许我们考虑如下一个退化的例子．设 X 是一个集合，那么函数 $X \to \varnothing$ 是什么呢？注意，$X \times \varnothing$ 的元素是序对 (x, y) 满足 $x \in X$，$y \in \varnothing$．由于不存在 $y \in \varnothing$，则不存在这样的序对，因此 $X \times \varnothing = \varnothing$．函数 $X \to \varnothing$ 是某种类型的 $X \times \varnothing$ 的子集，而 $X \times \varnothing = \varnothing$ 只有一个子集 $\varnothing$，因此 X 到 $\varnothing$ 至多有一个函数 $f=\varnothing$．函数 $X \to \varnothing$ 的定义要求对每个 $x \in X$，都存在唯一的 $y \in \varnothing$ 满足 $(x, y) \in f$．当 $X \neq \varnothing$ 时，存在 $x \in X$ 但不存在这样的 y（这是因为 $\varnothing$ 中没有元素 y），因此 f 不是函数．这样，当 $X \neq \varnothing$ 时，不存在 X 到 $\varnothing$ 的函数．另一方面，当 $X=\varnothing$ 时，我们断言 $f=\varnothing$ 是一个函数．否则，命题“f 是一个函数”的否命题将是真命题：“存在 $x \in \varnothing$，等等.”我们不必继续下去，因为 $\varnothing$ 中无任何元素．我们得出 $f=\varnothing$ 是函数 $\varnothing \to \varnothing$，并断言它就是恒等函数 $1_{\varnothing}$. ◀

对于其象等于整个目标域的函数有一个新的名称.

→ **定义** *称函数 $f: X \to Y$ 是*__*满射*__*（或到上的），若* $\operatorname{im} f = Y$.

因此，若对每个 $y \in Y$ 存在某个 $x \in X$（可能依赖 y）使得 $y=f(x)$，则 f 是满射.

例 2.4 (i)恒等函数是满射.

(ii)正弦函数 $\mathbb{R} \to \mathbb{R}$ 不是满射，因为它的象是 $[-1, 1]$，是目标域 $\mathbb{R}$ 的真子集.

(iii)函数 $x^2: \mathbb{R} \to \mathbb{R}$ 和 $e^x: \mathbb{R} \to \mathbb{R}$ 的目标域为 $\mathbb{R}$．因为 $\operatorname{im} x^2$ 由非负实数构成，$\operatorname{im} e^x$ 由正实数构成，所以 x^2 和 e^x 都不是满射.

(iv)设 $f: \mathbb{R} \to \mathbb{R}$ 定义为

$$f(a) = 6a + 4.$$

为弄清 f 是否是满射，我们要问是否每个 $b \in \mathbb{R}$ 有形式 $b=f(a)$，即给定 b，我们能否求出 a 使得

$$6a + 4 = b?$$ 90

我们总可以解这个关于 a 的方程，得到 $a=\frac{1}{6}(b-4)$．因此 f 是一个满射.

(v)设 f：$\mathbb{R} - \left\{\frac{3}{2}\right\} \to \mathbb{R}$ 定义为

$$f(a) = \frac{6a+4}{2a-3}.$$

为弄清 f 是否是满射，给定 b 去求解 a：我们能否总可以解

$$\frac{6a+4}{2a-3} = b?$$

由此得到方程 $a(6-2b)=-3b-4$，若 $6-2b\neq 0$，则可以解出 a[注意 $(-3b-4)/(6-2b)\neq 3/2$]. 另一方面，方程暗示当 $b=3$ 时无解，且事实上确实无解：若 $(6a+4)/(2a-3)=3$，交叉相乘得错误的方程 $6a+4=6a-9$. 因此，$3\notin \mathrm{im} f$，f 不是满射. ◀

有时我们不说函数 f 的值是唯一的，改说 f 是**单值的**. 例如，若 $\mathbb{R}^{\geqslant}$ 表示非负实数集，则 $\sqrt{\ }:\mathbb{R}^{\geqslant}\to\mathbb{R}^{\geqslant}$ 是函数，因为我们已经认为对每个正数 a 有 $\sqrt{a}\geqslant 0$. 另一方面，$f(a)=\pm\sqrt{a}$ 不是单值的，因而它不是函数.

证明一个被宣称为函数的 f 是否是单值的，最简单的办法是改述值的唯一性；用反证法叙述为

$$若\ a=a',\quad 则\ f(a)=f(a').$$

$g\left(\frac{a}{b}\right)=ab$ 定义了一个函数 $g:\mathbb{Q}\to\mathbb{Q}$ 吗？一个分数有许多种写法. 由于 $\frac{1}{2}=\frac{3}{6}$，可见 $g\left(\frac{1}{2}\right)=1\cdot 2\neq 3\cdot 6=g\left(\frac{3}{6}\right)$，所以 g 不是函数. 假若我们说只要 $\frac{a}{b}$ 是既约形式就有 $g\left(\frac{a}{b}\right)=ab$ 成立，那么 g 会是一个函数.

$f\left(\frac{a}{b}\right)=3\cdot\frac{a}{b}$ 确实定义了一个函数 $f:\mathbb{Q}\to\mathbb{Q}$，因为它是单值的：若 $\frac{a}{b}=\frac{a'}{b'}$，则 $f\left(\frac{a}{b}\right)=f\left(\frac{a'}{b'}\right)$. 为说明这一点，注意，由 $\frac{a}{b}=\frac{a'}{b'}$ 得 $ab'=a'b$，所以 $3ab'=3a'b$，$3\cdot\frac{a}{b}=3\cdot\frac{a'}{b'}$. 因此 f 是一个真正的函数.

下面的定义给出了函数的又一个重要性质.

→ **定义** *称函数 $f:X\to Y$ 是**单射**(或一对一的)，若只要 a 和 a' 是 X 的不同元素，则 $f(a)\neq f(a')$. 等价地说，(用反证法叙述)f 是单射，若对每对 a，$a'\in X$，我们有*

91

$$f(a)=f(a')\Rightarrow a=a'.$$

读者应当注意到，单射与单值在叙述上是互相颠倒的：f 是单值的，若 $a=a'\Rightarrow f(a)=f(a')$；$f$ 是单射，若 $f(a)=f(a')\Rightarrow a=a'$.

许多函数既不是单射也不是满射. 例如平方函数 $f:\mathbb{R}\to\mathbb{R}$，$f(x)=x^2$ 既不是单射也不是满射.

例 2.5 (i)恒等函数 1_X 是单射.

(ii)设 $f:\mathbb{R}-\left\{\frac{3}{2}\right\}\to\mathbb{R}$ 由下式定义：

$$f(a)=\frac{6a+4}{2a-3}.$$

为检验 f 是否是单射，假设 $f(a)=f(b)$：

$$\frac{6a+4}{2a-3}=\frac{6b+4}{2b-3}.$$

交叉相乘得

$$12ab+8b-18a-12=12ab+8a-18b-12,$$

这表明 $26a=26b$，因而 $a=b$. 所以得出 f 是单射的结论.（在例 2.4(v)中我们看见 f 不是满射.）

(iii)考虑 $f: \mathbb{R} \to \mathbb{R}$，$f(x)=x^2-2x-3$. 若我们想如(i)中那样通过观察 $f(a)=f(b)$ 的结果来检验 f 是否是单射，则会得到等式 $a^2-2a=b^2-2b$. 显然还不容易看出这个等式是否会导致 $a=b$. 我们转而求 $f(x)$ 的根，得到 3 和 -1. 于是 f 不是单射，因为 $f(3)=0=f(-1)$，即存在两个不同的数有相同的值. ◀

存在让两个函数合并形成另一个函数的方法，即它们的合成.

→ **定义** 若 $f: X \to Y$，$g: Y \to Z$ 都是函数(f 的目标域是 g 的定义域)，则它们的**合成**，记为 $g \circ f$，被定义为由下式给定的函数 $X \to Z$：

$$g \circ f: x \mapsto g(f(x)),$$

即先计算 f 在 x 处的值，再计算 g 在 $f(x)$ 处的值.

因此合成是一个两步过程：$x \mapsto f(x) \mapsto g(f(x))$. 例如，函数 $h: \mathbb{R} \to \mathbb{R}$，$h(x)=e^{\cos x}$ 是合成 $g \circ f$，其中 $f(x)=\cos x$，$g(x)=e^x$. 只要我们想计算，这种"分解"是很平常的，不妨计算 $h(\pi)$. 为计算 $h(\pi)$，我们必须先计算 $f(\pi)=\cos\pi=-1$，然后计算 $g(f(\pi))=g(-1)=e^{-1}$. 微积分中的链规则是一个用 g' 和 f' 计算导数 $(g \circ f)'$ 的公式： 92

$$(g \circ f)'(x) = g'(f(x)) \cdot f'(x).$$

若 $f: \mathbb{N} \to \mathbb{N}$，$g: \mathbb{N} \to \mathbb{R}$ 都是函数，则 $g \circ f: \mathbb{N} \to \mathbb{R}$ 有定义，但 $f \circ g$ 无定义[g 的目标 $=\mathbb{R} \neq \mathbb{N} = f$ 的定义域]. 甚至当 $f: X \to Y$ 和 $g: Y \to X$ 且两个合成 $g \circ f$ 和 $f \circ g$ 都有定义时，它们也不一定相等. 例如，定义 f，$g: \mathbb{N} \to \mathbb{N}$ 分别为 $f: n \mapsto n^2$ 和 $g: n \mapsto 3n$，则 $g \circ f: 2 \mapsto g(4)=12$，$f \circ g: 2 \mapsto f(6)=36$. 因而 $g \circ f \neq f \circ g$.

给定一个集合 X，设

$$\mathcal{F}(X) = \{\text{所有函数 } X \to X\}.$$

$\mathcal{F}(X)$ 中两个函数的合成总是有定义，而且合成也是 $\mathcal{F}(X)$ 中的函数. 正如我们刚才所看到的，这个乘法不交换，即 $f \circ g$ 和 $g \circ f$ 不一定相等. 下面我们证明合成总是满足结合律.

→ **引理 2.6** 函数的合成满足结合律：若

$$f: X \to Y, \quad g: Y \to Z, \quad \text{和} \quad h: Z \to W$$

都是函数，则

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

证明 我们证明两个合成在元素 $a \in X$ 处的值都是 $w=h(g(f(a)))$. 若 $x \in X$，则

$$h \circ (g \circ f): x \mapsto (g \circ f)(x) = g(f(x)) \mapsto h(g(f(x))) = w,$$

和

$$(h \circ g) \circ f: x \mapsto f(x) \mapsto (h \circ g)(f(x)) = h(g(f(x))) = w.$$

于是由命题 2.2 知这两个合成相等. ■

根据这个引理，我们没有必要写括号：记号 $h \circ g \circ f$ 的意思很清楚. 假设 $f: X \to Y$ 和 $g: Z \to W$ 都是函数. 若 $Y \subseteq Z$，则一些作者定义合成 $h: X \to W$ 为 $h(x)=g(f(x))$. 若 $Y \neq Z$，我们不允许有合成. 但是，我们可以定义 h 为合成 $h=g \circ i \circ f$，其中 $i: Y \to Z$ 是包含函数.

下面的结论表明，恒等函数 1_X 在 $\mathcal{F}(X)$ 中对合成所起的作用相当于 1 在数中对乘法所起的作用. 93

引理 2.7 设 $f: X \to Y$，则 $1_Y \circ f = f = f \circ 1_X$.

证明 设 $x \in X$，则

$$1_Y \circ f: x \mapsto f(x) \mapsto f(x)$$

和

$$f \circ 1_X: x \mapsto x \mapsto f(x). \qquad ■$$

在$\mathcal{F}(X)$中存在“倒数”吗？也就是说，对于函数 f，是否存在 $g \in \mathcal{F}(X)$使得 $f \circ g = 1_X$，$g \circ f = 1_X$？下面的讨论允许我们回答这个问题.

定义 *函数 $f: X \to Y$ 称为***双射***(或一一对应)，如果它既为单射又为满射.*

例 2.8 (i)恒等函数总是双射.

(ii)设 $X = \{1, 2, 3\}$，定义 $f: X \to X$ 为

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1.$$

容易看出 f 是双射. ◀

当 X 和 Y 都是有限集合时，我们可以用一个图表(如图 2-4 所示)把函数描绘出来. 设 $X = \{1, 2, 3, 4, 5\}$，$Y = \{a, b, c, d, e\}$，定义 $f: X \to Y$为

$$f(1) = b, \quad f(2) = e, \quad f(3) = a,$$
$$f(4) = b, \quad f(5) = c.$$

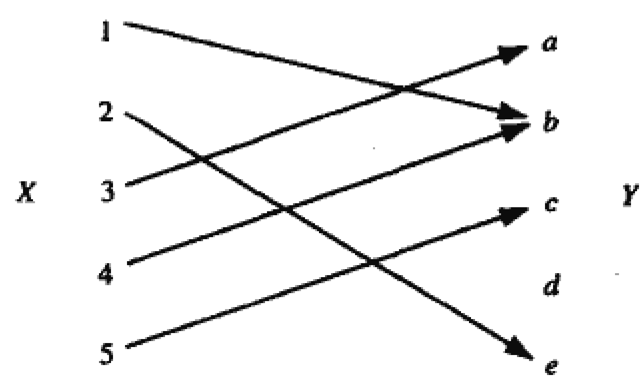


图 2-4 一个函数

因为 $f(1) = b = f(4)$，所以 f 不是单射；因为不存在 $x \in X$ 使 $f(x) = d$，所以 f 不是满射. 我们能
94 反转箭头得到映射 $g: Y \to X$ 吗？有两点可以说明不能得到. 第一，没有指向 d 的箭头，因此不能定义 $g(d)$. 第二，$g(b)$是 1 还是 4？第一个问题是 g 的定义域不是整个 Y，这是因为 f 不是满射；第二个问题是 g 不是单值的，这是因为 f 不是单射(这也说明了单射与单值在叙述上互相颠倒). 当 f 是双射时，这两个问题都不会产生.

定义 *函数 $f: X \to Y$ 有***反函数(或逆)***，如果存在函数 $g: Y \to X$ 使得合成$g \circ f$ 和 $f \circ g$ 都是恒等函数.*

我们不能说每个函数 f 都有反函数. 相反地，我们刚才已经分析了一些函数没有反函数的原因. 若反函数 g 存在，则 g 可以倒转图 2-4 中的箭头. 设 $f(a) = y$，则存在从 a 到 y 的箭头. 现在 $g \circ f$ 是恒等函数，因此 $a = (g \circ f)(a) = g(f(a)) = g(y)$. 这样 $g: y \mapsto a$，并且倒转 f 的描绘图表中的箭头就可以得到 g 的描绘图表. 若 f 转动什么东西，则它的反函数 g 就把它反转过来.

引理 2.9 *若函数 $f: X \to Y$ 和 $g: Y \to X$ 满足 $g \circ f = 1_X$，则 f 是单射且 g 是满射.*

证明 假设 $f(a) = f(a')$，则 $g(f(a)) = g(f(a'))$，即 $a = a'$[因为 $g(f(a)) = a$]，因此 f 是单射. 设 $x \in X$，则 $x = g(f(x))$，这样 $x \in \mathrm{im}\, g$，因此 g 是满射. ■

命题 2.10 *函数 $f: X \to Y$ 有反函数 $g: Y \to X$ 当且仅当 f 是双射.*

证明 若 f 有反函数g，则引理 2.9 表明 f 既是单射也是满射，因为 $g \circ f$ 和 $f \circ g$ 都是恒

等函数.

假设 f 是双射. 设 $y\in Y$. 因为 f 是满射，所以存在某个 $a\in X$ 使 $f(a)=y$. 又因为 f 是单射，所以这样的 a 是唯一的. 定义 $g(y)=a$，则 g 是一个(单值)函数，其定义域是 Y[g 只是"反转箭头"：因为 $f(a)=y$，所以存在 a 到 y 的箭头，且反转的箭头是从 y 到 a]. 显然 g 是 f 的反函数，即对所有 $y\in Y$ 有 $f(g(y))=f(a)=y$，对所有 $a\in X$ 都有 $g(f(a))=g(y)=a$. ■

记号 双射 f 的反函数记为 f^{-1}(由习题 2.9 知，一个函数不能有两个反函数). 在微积分中，反三角函数也使用相同的记号. 例如，$\sin^{-1}x=\arcsin x$，它满足 $\sin(\arcsin(x))=x$，$\arcsin(\sin(x))=x$. 当然，$\sin^{-1}$ 不能表示其倒数 $1/\sin x$，$1/\sin x=\csc x$. 95

例 2.11 我们可以找到两个函数 f 和 g 满足 $g\circ f$ 是恒等函数而 $f\circ g$ 不是恒等函数，因而 f 和 g 不互为反函数.

定义 f，g：$\mathbf{N}\to\mathbf{N}$ 如下：

$$f(n)=n+1;$$

$$g(n)=\begin{cases}0 & \text{当 } n=0\\ n-1 & \text{当 } n\geqslant 1.\end{cases}$$

合成 $g\circ f=1_{\mathbf{N}}$，因为 $g(f(n))=g(n+1)=n$(因为 $n+1\geqslant 1$). 另一方面，$f\circ g\neq 1_{\mathbf{N}}$，因为 $f(g(0))=f(0)=1\neq 0$. ◀

例 2.12 若 a 是实数，则用 a 乘是指函数 μ_a：$\mathbf{R}\to\mathbf{R}$，对所有 $r\in\mathbf{R}$ 有 $r\mapsto ar$. 若 $a\neq 0$，则 μ_a 是一个双射，其反函数叫做用 a 除，即 δ_a：$\mathbf{R}\to\mathbf{R}$，$r\mapsto \frac{1}{a}r$. 当然 $\delta_a=\mu_{1/a}$. 但是，若 $a=0$，则 $\mu_a=\mu_0$ 是常数函数 μ_0：$r\mapsto 0$，它没有反函数，因为它不是双射. ◀

有两个方法可确定一个给定的函数是否是双射：或者利用单射和满射的定义，或者求出它的反函数. 例如，若 $\mathbf{R}^+$ 表示正实数集，我们证明指数函数 f：$\mathbf{R}\to\mathbf{R}^+$，$f(x)=e^x=\sum x^n/n!$，是一个双射. 直接证明 f 是单射将要求证明若 $e^a=e^b$，则 $a=b$；直接证明 f 是满射将要求证明每个正实数 c 有形式 e^a. 用(自然)对数 $g(y)=\log y$ 证明这些命题是最简单的了. 常用公式 $e^{\log y}=y$ 和 $\log e^x=x$ 表明两个合成 $f\circ g$ 和 $g\circ f$ 都是恒等函数，所以 f 和 g 互为反函数. 因此，f 是双射，因为它有反函数.

让我们总结一下本节的结果.

→ **命题 2.13** 若集合 X 到自身的所有双射构成的集合记为 S_X，则函数的合成满足以下性质：

(i)若 f，$g\in S_X$，则 $f\circ g\in S_X$；

(ii)对所有 f，g，$h\in S_X$，$h\circ(g\circ f)=(h\circ g)\circ f$；

(iii)恒等函数 1_X 位于 S_X 中，且对每个 $f\in S_X$，有 $1_X\circ f=f=f\circ 1_X$；

(iv)对每个 $f\in S_X$，存在 $g\in S_X$，满足 $g\circ f=1_X=f\circ g$.

证明 我们只是重述了习题 2.14(ii)，引理 2.6、引理 2.7 和命题 2.10 的结果. ■ 96

以下是双射的一个有趣的应用. 容易证明(见习题 2.12)两个有限集 X 和 Y 有相同的元素个数当且仅当存在一个双射 f：$X\to Y$. 这暗示了下面的定义，它是康托尔(G. Cantor，1845—1918)提出的.

定义 两个集合(可能是无限集)X 和 Y **有相同的元素个数**，记为 $|X|=|Y|$，若存在一个双射 $f: X \to Y$.

例如，集合 X 称为**可数的**，若 X 是有限集或 X 和自然数集$\mathbb{N}$有相同的元素个数. 若 X 是无限可数的，则存在双射 $f: \mathbb{N} \to X$，即 X 的所有元素可以不重复地列出来 x_0，x_1，x_2，…，其中 $x_n=f(n)$，$n \in \mathbb{N}$. 康托尔证明了$\mathbb{R}$是**不可数的**，也就是说，$\mathbb{R}$ 不是可数的. 这样，无限集有不同的大小(实际上，无限集有无限多个不同的大小). 大小的不同是有用的. 例如，实数 z 称为**代数数**，如果它是某个多项式 $f(x)=q_0+q_1x+\cdots+q_nx^n$的根，其中系数$q_0$，$q_1$，…，$q_n$ 都是有理数；实数 z 称为**超越数**，如果它不是代数数. 当然，每个有理数 r 都是代数数，因为它是 $x-r$ 的根. 无理数中也存在代数数，例如，$\sqrt{2}$是代数数，因为它是 x^2-2 的根. 那么是否有超越数呢？我们可以证明仅存在可数个代数数，于是由康托尔定理中$\mathbb{R}$ 的不可数性知，存在(不可数多个)超越数.

注 为什么当函数的象更重要时我们关心的却是函数的目标域？从可行性来说，当第一次定义函数时，我们通常不知道它的象. 例如，设 $f: \mathbb{R} \to \mathbb{R}$ 被定义为

$$f(x)=|x|^{e^{-x}}\sqrt[5]{x^2+\sin^2 x}.$$

我们必须分析 f 以求出它的象，而且这不是一个小任务. 但是，若目标域必须是象，则我们甚至不能写 $f: X \to Y$，因为还没有首先求出 f 的象. 因此，目标域用起来更方便.

函数相等的定义的一部分是它们的目标域相等，改变目标域就改变了函数. 假设我们没有这样做. 考虑函数 $f: X \to Y$，且它不是满射，设 $Y'=\operatorname{im} f$，并定义 $g: X \to Y'$，对所有 $x \in X$ 有 $g(x)=f(x)$. 函数 f 和 g 有相同的定义域和相同的值(即相同的图像)，它们只有目标域不同. 现在 g 是满射. 假如我们认为目标域在函数的定义中不是必要的因素，则可以区分 f 和 g，因为 f 不是满射，g 是满射. 于是每个函数都是满射(这不会动摇数学的根本，但是会迫使我们利用累赘的句子进行说明). 习
97 题 4.26说明了使用目标域的更实际的理由.

设 X，Y 都是集合，则函数 $f: X \to Y$ 定义了一个“向前移动”，把 X 的子集移入 Y 的子集：若 $S \subseteq X$，则

$$f(S)=\{y \in Y: \text{对某个 } s \in S, y=f(s)\}.$$

我们称 $f(S)$为 S 的**直接象**. 函数 f 也定义了一个“向后移动”，把 Y 的子集移入 X 的子集：若 $W \subseteq Y$，则

$$f^{-1}(W)=\{x \in X: f(x) \in W\}.$$

我们没有假设 f 是双射，所以这里 f^{-1}并不是指反函数. $f^{-1}(W)$是指由 X 中所有那些被 f 送进 W 中的元素构成的集合，如果有的话. 我们称 $f^{-1}(W)$为 W 的**逆象**.

习题 2.16 已经证明了直接象保持并的不变：若 $f: X \to Y$，且$\{S_i : i \in I\}$是 X 的一族子集，则 $f\left(\bigcup_{i \in I} S_i\right)=\bigcup_{i \in I} f(S_i)$. 另一方面，$f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$是可能的. 习题 2.17 表明逆象比直接象性质更好.

命题 2.14 设 X，Y 都是集合，$f: X \to Y$ 是一个函数.

(i)若 $T\subseteq S$ 都是 X 的子集，则 $f(T)\subseteq f(S)$，且若 $U\subseteq V$ 都是 Y 的子集，则 $f^{-1}(U)\subseteq f^{-1}(V)$.

(ii)若 $U\subseteq Y$，则 $ff^{-1}(U)\subseteq U$；若 f 是一个满射，则 $ff^{-1}(U)=U$.

(iii)若 $T\subseteq X$，则 $T\subseteq f^{-1}f(T)$；若 f 是一个单射，则 $W=f^{-1}f(T)$.

证明 (i)若 $y\in f(T)$，则对某个 $t\in T$ 有 $y=f(t)$. 但是因为 $T\subseteq S$，所以 $t\in S$，所以 $f(t)\in f(S)$. 因此 $f(T)\subseteq f(S)$. 另一个包含关系可类似证得.

(ii)若 $a\in ff^{-1}(U)$，则对某个 $x'\in f^{-1}(U)$有 $a=f(x')$，即 $a=f(x')\in U$. 当 f 是满射时证明相反的包含关系成立. 若 $u\in U$，则存在 $x\in X$ 使得 $f(x)=u$，因而 $x\in f^{-1}(U)$，所以 $u=f(x)\in ff^{-1}(U)$.

(iii)若 $t\in T$，则 $f(t)\in f(T)$，所以 $t\in f^{-1}f(t)\subseteq f^{-1}(T)$. 当 f 是单射时我们证明相反的包含关系成立. 若 $x\in f^{-1}f(T)$，则 $f(x)\in f(T)$，因而存在 $t\in T$ 使 $f(x)=f(t)$. 由于 f 是一个单射，所以 $x=t$，$x\in T$. ■

命题 2.14(ii)中的严格不等号可能成立. 若 $f: \mathbb{Z}\to\mathbb{Q}$ 是包含函数，则

$$ff^{-1}\left(\left\{\frac{1}{2}\right\}\right)=f(\varnothing)=\varnothing\subsetneq\left\{\frac{1}{2}\right\}.$$

命题 2.14(iii)中的严格不等号也可能成立. 设 $f: \mathbb{R}\to S^1$ 被定义为 $f(x)=e^{2\pi i x}$，其中 S^1 是单位圆. 若 $A=\{0\}$，则 $f(A)=\{1\}$且

$$f^{-1}f(A)=f^{-1}f(\{0\})=f^{-1}(\{1\})=\mathbb{Z}\supsetneq A.$$ 98

推论 2.15 若 $f: X\to Y$ 是满射，则$\mathcal{P}(Y)\to\mathcal{P}(X)$，$B\mapsto f^{-1}(B)$是一个单射，其中$\mathcal{P}(Y)$表示由 Y 的所有子集构成的族.

证明 若 B，$C\subseteq Y$ 且 $f^{-1}(B)=f^{-1}(C)$，则由命题 2.14(ii)知

$$B=ff^{-1}(B)=ff^{-1}(C)=C.$$ ■

→2.1.2 等价关系

我们将定义一个重要的概念——等价关系，但是先从关系的一般概念开始.

→ **定义** 给定集合 X 与 Y，X 到 Y 的一个关系是指 $X\times Y$ 的一个子集 R. 若 $X=Y$，则我们说 R 是 X 上的一个关系. 我们通常写成 xRy，而不写成$(x, y)\in R$.

以下是一个具体的例子. 当然，$\leqslant$应当是$\mathbb{R}$上的一个关系. 为看出这一点，定义关系

$$R=\{(x,y)\in\mathbb{R}\times\mathbb{R}:(x,y)\text{ 在直线 } y=x \text{ 上或者上方}\}.$$

读者应当验证 $x\leqslant y$ 当且仅当$(x, y)\in R$.

例 2.16 (i)每个函数 $f: X\to Y$ 是 X 到 Y 的一个关系.

(ii)相等是任何集合 X 上的一个关系.

(iii)mod m 同余是$\mathbb{Z}$上的一个关系. ◀

→ **定义** 集合 X 上的一个关系 $x\equiv y$ 是

自反的：对所有 $x\in X$ 有 $x\equiv x$；

对称的：对所有 x，$y\in X$，若 $x\equiv y$，则 $y\equiv x$；

传递的：对所有 x，y，$z\in X$，若 $x\equiv y$ 和 $y\equiv z$，则 $x\equiv z$.

若 X 上的一个关系具有三条性质：自反性，对称性和传递性，则称该关系为 X 上的一个
99 **等价关系**.

例 2.17 (i)普通的相等关系是任意集合上的一个等价关系.

(ii)若 $m\geqslant 0$，则命题 1.57 是说 $x\equiv y \bmod m$ 是 $X=\mathbb{Z}$ 上的一个等价关系.

(iii)设 $X=\{(a, b)\in \mathbb{Z}\times\mathbb{Z}: b\neq 0\}$，并定义 X 上的一个关系≡为交叉相乘：

$$(a,b)\equiv(c,d) \quad 当 \quad ad=bc.$$

我们断言≡是一个等价关系. 自反性和对称性的验证是很容易的. 对于传递性，假设 $(a, b)\equiv(c, d)$，$(c, d)\equiv(e, f)$. 由 $ad=bc$ 得 $adf=bcf$，由 $cf=de$ 得 $bcf=bde$，因此 $adf=bde$. 我们可以消去非零整数 d 得 $af=be$，即 $(a, b)\equiv(e, f)$.

(iv)在微积分中，等价关系隐含在对向量的讨论中. 从点 P 到点 Q 的一个箭头可以用有序对 (P, Q) 表示，称 P 是它的起点，Q 是它的终点. 箭头上的一个等价关系可以被定义为：若箭头 (P, Q) 和 (P', Q') 有相同的长度和方向则 $(P, Q)\equiv(P', Q')$. ◀

集合 X 上的一个等价关系产生 X 的一族子集.

→ **定义** 设≡是集合 X 上的一个等价关系. 若 $a\in X$，则 a 的**等价类**，记为 $[a]$，定义为

$$[a]=\{x\in X: x\equiv a\}\subseteq X.$$

现在描述由上面等价关系产生的等价类.

→ **例 2.18** (i)设≡是集合 X 上的相等关系. 若 $a\in X$，则 $[a]=\{a\}$ 是只含一个元素 a 的子集. 毕竟，若 $x=a$，则 x 和 a 相等！

(ii)考虑 $\mathbb{Z}$ 上的模 m 同余关系，设 $a\in\mathbb{Z}$. a 的**同余类**定义为

100 $$\{x\in\mathbb{Z}: x=a+km, k\in\mathbb{Z}\}.$$

另一方面，根据定义，a 的等价类是

$$\{x\in\mathbb{Z}: x\equiv a \bmod m\}.$$

由于 $x\equiv a \bmod m$ 当且仅当对某个 $k\in\mathbb{Z}$ 有 $x=a+km$，所以这两个子集是一致的，即等价类 $[a]$ 是同余类.

(iii)在交叉相乘下 (a, b) 的等价类是

$$[(a,b)]=\{(c,d): ad=bc\}.$$

其中 a，$b\in\mathbb{Z}$ 且 $b\neq 0$. 若我们记 $[(a, b)]$ 为 a/b，则这个等价类正是通常被记为 a/b 的分数. 毕竟，$(1, 2)\neq(2, 4)$ 是显然的，但是 $[(1, 2)]=[(2, 4)]$，即 $1/2=2/4$.

(iv)在例 2.17(iv)中，箭头的等价类 $[(P, Q)]$ 称为一个**向量**，我们记它为 $[(P, Q)]=\overrightarrow{PQ}$. ◀

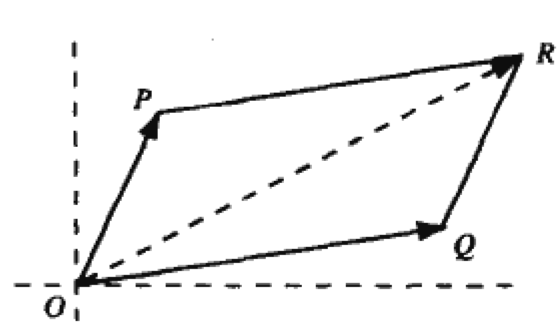


图 2-5 平行四边形法则

比较有理数和向量是有意义的，因为它们都被定义为等价类. 每个有理数 a/b 有一个"可爱的"名字：既约表达式. 每个向量有一个可爱的名字：起点在原点处的箭头 (O, Q). 分数用既约表达式并不总是很方便的. 例如，即使 a/b 和 c/d 都是既约形式，它们的和 $(ad+bc)/bd$ 也不一定是既约形式. 向量加法由平行四边形法则定义(见图 2-5)：$\overrightarrow{OP}+\overrightarrow{OQ}=\overrightarrow{OR}$，其中 O，P，Q 和 R 都是平行四边形的顶

点. 因为$(O, Q)\equiv(P, R)$，所以$\overrightarrow{OQ}=\overrightarrow{PR}$，所以$\overrightarrow{OP}+\overrightarrow{OQ}=\overrightarrow{OP}+\overrightarrow{PR}=\overrightarrow{OR}$更自然些.

→ **引理 2.19** *若$\equiv$是集合 X 上的一个等价关系，则 $x\equiv y$ 当且仅当$[x]=[y]$.*

证明 假设 $x\equiv y$. 若 $z\in[x]$，则 $z\equiv x$，由传递性得 $z\equiv y$. 因而$[x]\subseteq[y]$. 根据对称性，$y\equiv x$，由此得反包含$[y]\subseteq[x]$. 因此$[x]=[y]$. 101

反之，若$[x]=[y]$，则根据自反性，$x\in[x]$，所以 $x\in[x]=[y]$，因此 $x\equiv y$. ■

总之，这个引理是说：在用等价类代替元素的条件下我们可以用相等代替等价.

以下是一个集合论思想，我们将证明它本质上包含着等价关系.

→ **定义** *集合 X 的一族子集$\mathcal{P}$称为***两两不相交**，*若对所有 $A, B\in\mathcal{P}$，有 $A=B$ 或 $A\cap B=\varnothing$.*

集合 X 的一个**分类**是指：一族非空的两两不相交的子集(称为**块**)，并且它们的并是 X.

注意到，若 X 是一个有限集，且 $A_1, A_2, \cdots, A_n$ 是 X 的一个分类，则

$$|X|=|A_1|+|A_2|+\cdots+|A_n|.$$

我们将证明等价关系和分类只是同一事物的不同看法.

→ **命题 2.20** *若$\equiv$是集合 X 上的一个等价关系，则等价类构成 X 的一个分类. 反之，给定 X 的一个分类$\mathcal{P}$，则存在 X 上的一个等价关系，其等价类是$\mathcal{P}$中的块.*

证明 假设 X 上的一个等价关系$\equiv$已给定. 因为$\equiv$是自反的，所以每个 $x\in X$ 位于等价类$[x]$中. 于是等价类是非空的子集，并且它们的并为 X. 为证明两两不相交，假设 $a\in[x]\cap[y]$，则 $a\equiv x$，$a\equiv y$. 根据对称性，$x\equiv a$，由传递性得 $x\equiv y$. 因此根据引理 2.19，有$[x]=[y]$，所以等价类构成 X 的一个分类.

反之，设$\mathcal{P}$是 X 的一个分类. 设 $x, y\in X$，若存在 $A\in\mathcal{P}$可使 $x\in A$ 和 $y\in A$，则定义 $x\equiv y$. 显然$\equiv$是自反的和对称的. 为看出$\equiv$是传递的，假设 $x\equiv y$ 和 $y\equiv z$，即存在 $A, B\in\mathcal{P}$ 使 $x, y\in A$ 和 $y, z\in B$. 由于 $y\in A\cap B$，由两两不相交得 $A=B$，所以 $x, z\in A$，即 $x\equiv z$. 我们已经证明了$\equiv$是一个等价关系.

最后证明等价类是$\mathcal{P}$中的子集. 若 $x\in X$，则对某个 $A\in\mathcal{P}$有 $x\in A$. 根据$\equiv$的定义，若 $y\in A$，则 $y\equiv x$ 和 $y\in[x]$，因而 $A\subseteq[x]$. 对于反包含，设 $z\in[x]$，则 $z\equiv x$. 存在某个 B 满足 $x\in B$ 和 $z\in B$，因此 $x\in A\cap B$. 根据两两不相交有 $A=B$，所以 $z\in A$，$[x]\subseteq A$. 因此$[x]=A$. ■ 102

例 2.21 (i)若$\equiv$是集合 X 上的恒等关系，则块是 X 的 1-点子集.

(ii)设 $X=[0, 2\pi]$，并定义 X 的分类，其块为$\{0, 2\pi\}$和单点集$\{x\}$，其中 $0<x<2\pi$. 这个分类决定了区间的端点(没有其他的)，所以我们可以把它当作单位圆的一个构造. ◀

给定集合 X 上的一个等价关系，构造集合 $\widetilde{X}$ 使其元素是 $x\in X$ 的等价类$[x]$，这是一个很平常的做法. 例如，在例 2.17(iii)中，我们有 $X=\{(a, b)\in\mathbb{Z}\times\mathbb{Z} : b\neq 0\}$ 和 $\widetilde{X}=\mathbb{Q}$. 如果我们想定义一个函数，就必须保证它是单值的，特别地，当定义域是 $\widetilde{X}$ 时，也是这样的. 我们已经知道 $f(a/b)=ab$ 不能定义函数$\mathbb{Q}\to\mathbb{Z}$，这是因为它的值依赖于等价类$[(a, b)]=a/b$ 中代表(a, b)的选择. 相反地，有理数的加法，$\alpha : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$，$(a/b)+(c/d)=(ad+bd)/bd$，定义了一个函数. 有理数的加法不依赖于代表的选择. 读者可以证明，若 $a/b=a'/b'$ 和 $c/d=c'/d'$，则$(ad+bc)/bd=(a'd'+b'c')/b'd'$. 在声明 f 是一个(单值的)函数之前，我们必须证明它的值与代表的选择无关. 若检验了一个定义域为 $\widetilde{X}$ 的函数 f 是单值的，则称 f 是**定义良好的**.

习题

H 2.1 判断对错并说明理由.

(i)若 $S\subseteq T$，$T\subseteq X$，则 $S\subseteq X$.

(ii)任意两个函数 $f: X\to Y$ 和 $g: Y\to Z$ 都有一个合成 $f\circ g: X\to Z$.

(iii)任意两个函数 $f: X\to Y$ 和 $g: Y\to Z$ 都有一个合成 $g\circ f: X\to Z$.

(iv)对每个集合 X 都有 $X\times\varnothing=\varnothing$.

(v)若 $f: X\to Y$ 和 $j: \mathrm{im} f\to Y$ 都是包含映射，则存在一个满射 $g: X\to \mathrm{im} f$ 满足 $f=j\circ g$.

(vi)若 $f: X\to Y$ 是一个函数，且存在函数 $g: Y\to X$ 满足 $f\circ g=1_Y$，则 f 是一个双射.

(vii)$f\left(\frac{a}{b}\right)=(a+b)(a-b)$是一个定义良好的函数$\mathbb{Q}\to\mathbb{Z}$.

(viii)若 $f: \mathbb{N}\to\mathbb{N}$，$f(n)=n+1$，$g: \mathbb{N}\to\mathbb{N}$，$g(n)=n^2$，则合成 $g\circ f$ 是 $n\mapsto n^2(n+1)$.

(ix)复共轭 $z=a+ib\mapsto \bar{z}=a-ib$ 是一个双射$\mathbb{C}\to\mathbb{C}$.

103 2.2 设 A，B 都是集合 X 的子集，证明 $A-B=A\cap B'$，其中 $B'=X-B$ 是 B 的补集.

*2.3 设 A，B 都是集合 X 的子集，证明下列**模律**：

$$(A\cup B)'=A'\cap B' \quad 和 \quad (A\cap B)'=A'\cup B',$$

其中 $A'=X-A$ 表示 A 的补集.

*2.4 设 A，B 都是集合 X 的子集，定义它们的**对称差**(见图 2-6)为

$$A+B=(A-B)\cup(B-A).$$

(i)证明 $A+B=(A\cup B)-(A\cap B)$.

(ii)证明 $A+A=\varnothing$.

(iii)证明 $A+\varnothing=A$.

H (iv)证明 $A+(B+C)=(A+B)+C$(见图 2-7).

(v)证明 $A\cap(B+C)=(A\cap B)+(A\cap C)$.

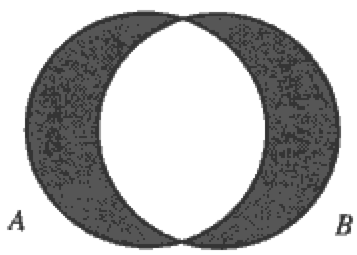


图 2-6 对称差

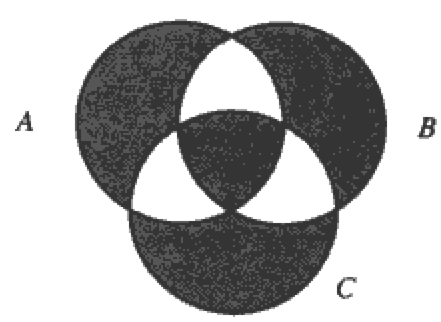


图 2-7 结合律

*2.5 设 A，B 都是集合，并设 $a\in A$，$b\in B$. 定义它们的**有序对**如下：

$$(a,b)=\{a,\{a,b\}\}.$$

若 $a'\in A$，$b'\in B$，证明$(a', b')=(a, b)$当且仅当 $a'=a$ 和 $b'=b$.

2.6 设 $\Delta=\{(x, x): x\in\mathbb{R}\}$，因此 Δ 是平面上的一条直线，它过原点并将 x 轴旋转了 45°.

H (i)若 $P=(a, b)$是平面上满足 $a\neq b$ 的一点，证明 Δ 是端点为 $P=(a, b)$和 $P'=(b, a)$的线段 PP'的垂直平分线.

(ii)若 $f: \mathbb{R}\to\mathbb{R}$ 是一个双射，其图像由某些点(a, b)构成[当然，$b=f(a)$]，证明 f^{-1}的图像是$\{(b, a): (a, b)\in f\}$.

*2.7 设 X，Y 都是集合，$f: X\to Y$ 是一个函数.

H (i)若 S 是 X 的一个子集，证明限制 $f|S$ 等于合成 $f\circ i$，其中 $i:S\to X$ 是包含映射.

(ii)若 $\mathrm{im}f=A\subseteq Y$，证明存在一个满射 $f':X\to A$ 满足 $f=j\circ f'$，其中 $j:A\to Y$ 是包含映射. 104

H 2.8　若 $f:X\to Y$ 有反函数 g，证明 g 是一个双射.

*2.9　证明，若 $f:X\to Y$ 是一个双射，则它恰有一个反函数.

H 2.10　证明 $f:\mathbf{R}\to\mathbf{R}$，$f(x)=3x+5$ 是一个双射，并求出它的反函数.

H 2.11　判断 $f:\mathbf{Q}\times\mathbf{Q}\to\mathbf{Q}$，$f(a/b,c/d)=(a+c)/(b+d)$ 是否是一个函数.

*H 2.12　设 $X=\{x_1,\cdots,x_m\}$，$Y=\{y_1,\cdots,y_n\}$ 都是有限集，其中 x_i 都是不同的，且 y_j 也都是不同的. 证明 $f:X\to Y$ 是一个双射当且仅当 $|X|=|Y|$，即 $m=n$.

*2.13　(鸽巢原理)

H (i)若 X，Y 都是有限集，且元素个数相同，对函数 $f:X\to Y$，证明下述条件是等价的：

(i) f 是单射；

(ii) f 是双射；

(iii) f 是满射.

(ii)假设有 11 只鸽子，每只鸽子都在某个鸽巢中. 若只有 10 个鸽巢，证明有一个鸽巢中的鸽子数超过 1.

*2.14　设 $f:X\to Y$ 和 $g:Y\to Z$ 都是函数.

(i)若 f，g 都是单射，证明 $g\circ f$ 是单射.

(ii)若 f，g 都是满射，证明 $g\circ f$ 是满射.

(iii)若 f，g 都是双射，证明 $g\circ f$ 是双射.

(iv)若 $g\circ f$ 是双射，证明 f 是单射，g 是满射.

2.15　H (i)证明，若 $f:(-\pi/2,\pi/2)\to\mathbf{R}$，$a\mapsto\tan a$，则 f 有反函数 g，事实上 $g=\arctan$.

(ii)证明 $\arcsin x$ 和 $\arccos x$ 都是本节定义的反函数(分别是 $\sin x$ 和 $\cos x$ 的). (定义域和目标域必须要小心选择.)

*2.16　(i)设 $f:X\to Y$ 是一个函数，$\{S_i:i\in I\}$ 是 X 的一族子集. 证明

$$f\Big(\bigcup_{i\in I}S_i\Big)=\bigcup_{i\in I}f(S_i).$$

(ii)若 S_1，S_2 都是集合 X 的子集，且 $f:X\to Y$ 是一个函数，证明 $f(S_1\cap S_2)\subseteq f(S_1)\cap f(S_2)$. 给出满足 $f(S_1\cap S_2)\neq f(S_1)\cap f(S_2)$ 的一个例子.

(iii)若 S_1，S_2 都是集合 X 的子集，且 $f:X\to Y$ 是一个单射，证明 $f(S_1\cap S_2)=f(S_1)\cap f(S_2)$.

*2.17　设 $f:X\to Y$ 是一个函数.

(i)若 $B_i\subseteq Y$ 是 Y 的一族子集，证明

$$f^{-1}\Big(\bigcup_i B_i\Big)=\bigcup_i f^{-1}(B_i)\quad 和\quad f^{-1}\Big(\bigcap_i B_i\Big)=\bigcap_i f^{-1}(B_i).$$ 105

(ii)若 $B\subseteq Y$，证明 $f^{-1}(B')=f^{-1}(B)'$，其中 B' 表示 B 的补集.

2.18　设 $f:X\to Y$ 是一个函数. 定义 X 上的一个关系：若 $f(x)=f(x')$，则 $x\equiv x'$. 证明 $\equiv$ 是一个等价关系. 若 $x\in X$ 且 $f(x)=y$，则等价类 $[x]$ 记为 $f^{-1}(y)$，称为 y 上的纤维.

2.19　设 $X=\{$石头，纸，剪刀$\}$. 回忆游戏规则：纸赢石头，石头赢剪刀，剪刀赢纸. 画出 $X\times X$ 的一个子集，以表明赢是 X 上的一个关系.

2.20　H (i)下面这个命题声称证明了集合 X 上满足对称性和传递性的关系 R 一定有自反性，即 R 是 X 上的一个等价关系，请找出其中的错误. 若 $x\in X$ 且 xRy，则由对称性得 yRx，由传递性得 xRx.

(ii)给一个例子，表明单位闭区间 $X=[0,1]$ 上满足对称性和传递性的关系不满足自反性.

→2.2 置换

→ **定义** 设 X 是一个集合，则 X 中的一个**表**是指函数 $f:\{1, 2, \cdots, n\}\to X$. 若 X 中的表 f 是双射(因而 X 是一个有限集，且 $|X|=n$)，则称 f 为 X 的一个**排列**.

若 f 是一个表，则记它的值 $f(i)$ 为 x_i，其中 $1\leqslant i\leqslant n$. 因此，X 中的表只是一个 n-元组 $(x_1, x_2, \cdots, x_n)$. 说表 f 是单射，就是说不存在重复的坐标[若 $i\neq j$，则 $x_i=f(i)\neq f(j)=x_j$]. 说 f 是满射，就是说每个 $x\in X$ 作为某个坐标出现. 因此，X 的排列是 X 的所有元素组成的一个无重复的 n-元组 $(x_1, x_2, \cdots, x_n)$. 我们通常省略圆括号，把表写成 $x_1, x_2, \cdots, x_n$. 例如，$X=\{a, b, c\}$ 有 27 个表和 6 个排列：

$$abc;\quad acb;\quad bac;\quad bca;\quad cab;\quad cba.$$

对这些表，我们要做的事情是数一下它们有多少个. 一个 n-元集合 X 恰有 n^n 个表和 $n!$ 个排列.

→ **定义** 设 X 是一个集合(可能是无限集)，X 的一个**置换**是指双射 $\alpha: X\to X$.

给定一个有限集 X，$|X|=n$，设 $\varphi:\{1, 2, \cdots, n\}\to X$ 是一个排列. 当然，φ 是一个双射. 若 $f:\{1, 2, \cdots, n\}\to X$ 是 X 的一个排列，则 $f\circ\varphi^{-1}: X\to X$ 是 X 的一个置换. 反之，
106 若 $\alpha: X\to X$ 是 X 的一个置换，则 $\alpha\circ\varphi:\{1, 2, \cdots, n\}\to X$ 是 X 的一个排列. 因此排列和置换只是描述同一事物的两种不同方法. 使用置换而不使用排列，其好处是置换可以作合成运算，且由习题 2.14(ii)知，它们的合成也是置换.

若 $X=\{1, 2, \cdots, n\}$，则我们可以使用一个二行记号来表示置换 α：

$$\alpha=\begin{pmatrix}1 & 2 & \cdots & j & \cdots & n\\ \alpha(1) & \alpha(2) & \cdots & \alpha(j) & \cdots & \alpha(n)\end{pmatrix}$$

因此底行是排列 $\alpha(1), \alpha(2), \cdots, \alpha(n)$.

这一节的大多数结果首次出现在 1815 年柯西(Cauchy)的一篇论文中(见图 2-9).

→ **定义** 集合 X 的所有置换构成的族，记为 S_X，称为 X 上的**对称群**. 当 $X=\{1, 2, \cdots, n\}$ 时，S_X 通常记为 S_n，并称为 n **次对称群**.

注意：S_3 中的合成不交换. 若

$$\alpha=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\quad 和\quad \beta=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},$$

则它们的合成[⊖]是

$$\alpha\circ\beta=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\quad 和\quad \beta\circ\alpha=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

因此 $\alpha\circ\beta: 1\mapsto\alpha(\beta(1))=\alpha(2)=3$，而 $\beta\circ\alpha: 1\mapsto 2\mapsto 1$，所以 $\alpha\circ\beta\neq\beta\circ\alpha$.

另一方面，有些置换是交换的. 例如，

⊖ 有些作者做置换乘法的方法不同，他们的 $\alpha\circ\beta$ 是我们的 $\beta\circ\alpha$. 详细地说，设 $\alpha, \beta: X\to X$. 由于我们写 α 在 $i\in X$ 处的值为 $\alpha(i)$，所以先应用 α 再应用 β 的合成为：$i\mapsto\alpha(i)\mapsto\beta(\alpha(i))$. 因此我们自然会记这个先 α 后 β 的合成为 $\beta\circ\alpha$. 但是，有些作者是使用一套右边记号，他们记 α 在 i 处的值为 $(i)\alpha$. 对他们来说，先 α 后 β 是：$i\mapsto(i)\alpha\mapsto((i)\alpha)\beta$. 所以记这个合成为 $\alpha\circ\beta$，即我们的 $\beta\circ\alpha$ 是他们的 $\alpha\circ\beta$. 我们将总是写 $\beta\circ\alpha$ 来表示先 α 后 β，但是读者应当知道其他书可能使用右边记号.

$$\gamma=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\quad 和 \quad \delta=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$$

交换，读者可以验证之.

S_X 中的合成满足消去律：

$$若\ \gamma\circ\alpha=\gamma\circ\beta,\quad 则\quad \alpha=\beta.$$ 107

这是因为，

$$\begin{aligned}\alpha&=1_X\circ\alpha\\&=(\gamma^{-1}\circ\gamma)\circ\alpha\\&=\gamma^{-1}\circ(\gamma\circ\alpha)\\&=\gamma^{-1}\circ(\gamma\circ\beta)\\&=(\gamma^{-1}\circ\gamma)\circ\beta\\&=1_X\circ\beta=\beta.\end{aligned}$$

类似的讨论可证明

$$\alpha\circ\gamma=\beta\circ\gamma\Rightarrow\alpha=\beta.$$

用二行记号表示置换除了显得麻烦之外，还存在一个主要问题. 对诸如：一个置换的平方是恒等函数吗？使一个置换的 m 次幂为恒等函数的正整数 m 最少取多少？我们可以把一个置换分解成更简单的置换吗？这样的初等问题，它隐藏了回答. 以下介绍的特殊置换将弥补这个缺陷.

我们先简化一些记号，$\beta\circ\alpha$ 记为 $\beta\alpha$，1_X 记为(1).

→ **定义** 设 $\alpha\in S_n$，$i\in\{1, 2, \cdots, n\}$，若 $\alpha(i)=i$，则称 α **固定** i，若 $\alpha(i)\neq i$，则称 α **移动** i.

→ **定义** 设 $\alpha\in S_n$ 且 $i_1, i_2, \cdots, i_r$ 是 $\{1, 2, \cdots, n\}$ 中的不同整数. 若

$$\alpha(i_1)=i_2,\alpha(i_2)=i_3,\cdots,\alpha(i_{r-1})=i_r,\alpha(i_r)=i_1,$$

且 α 固定其他整数(如果还有的话)，则称 α 为一个 r-**循环置换**. 我们也可以说 α 是一个**长度为** r 的循环置换.

一个 2-循环置换交换 i_1 和 i_2 并固定其他整数. 2-循环置换也称为**对换**. 1-循环置换是恒等函数，因为它固定每个 i. 因此，所有 1-循环置换都是相等的：对所有 i 有 $(i)=(1)$.

考虑下面的置换

$$\alpha=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}.$$

二行记号不能帮助我们认识到 α 实际上是一个 5-循环置换：$\alpha(1)=4$，$\alpha(4)=5$，$\alpha(5)=2$，$\alpha(2)=3$，$\alpha(3)=1$. 现在我们引入一个新的记号：如定义所述，一个 r-循环置换 α 被记为

$$\alpha=(i_1 i_2\cdots i_r).$$ 108

例如，上述 5-循环置换 α 被记为 $\alpha=(1\ 4\ 5\ 2\ 3)$. 读者可以验证

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1\ 2\ 3\ 4),$$

$$\begin{pmatrix}1&2&3&4&5\\5&1&4&2&3\end{pmatrix}=(1\ 5\ 3\ 4\ 2),$$

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}=(1\ 2\ 3).$$

注意

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

不是一个循环置换，实际上，$\beta=(1\ 2)(3\ 4)$．术语“循环置换(cycle)”来自单词 circle 的希腊词．我们可以把循环置换$(i_1 i_2 \cdots i_r)$当作圆周的一个顺时针旋转，如图 2-8 所示．任意 i_j 可以被取为“出发点”，因此任意 r-循环置换有 r 个不同的记法：

$$(i_1 i_2 \cdots i_r) = (i_2 i_3 \cdots i_r i_1) = \cdots = (i_r i_1 i_2 \cdots i_{r-1}).$$

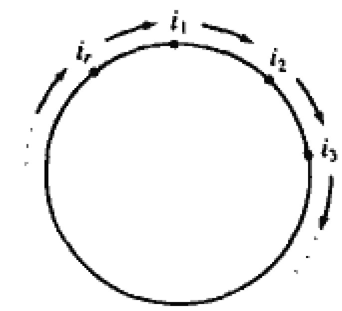
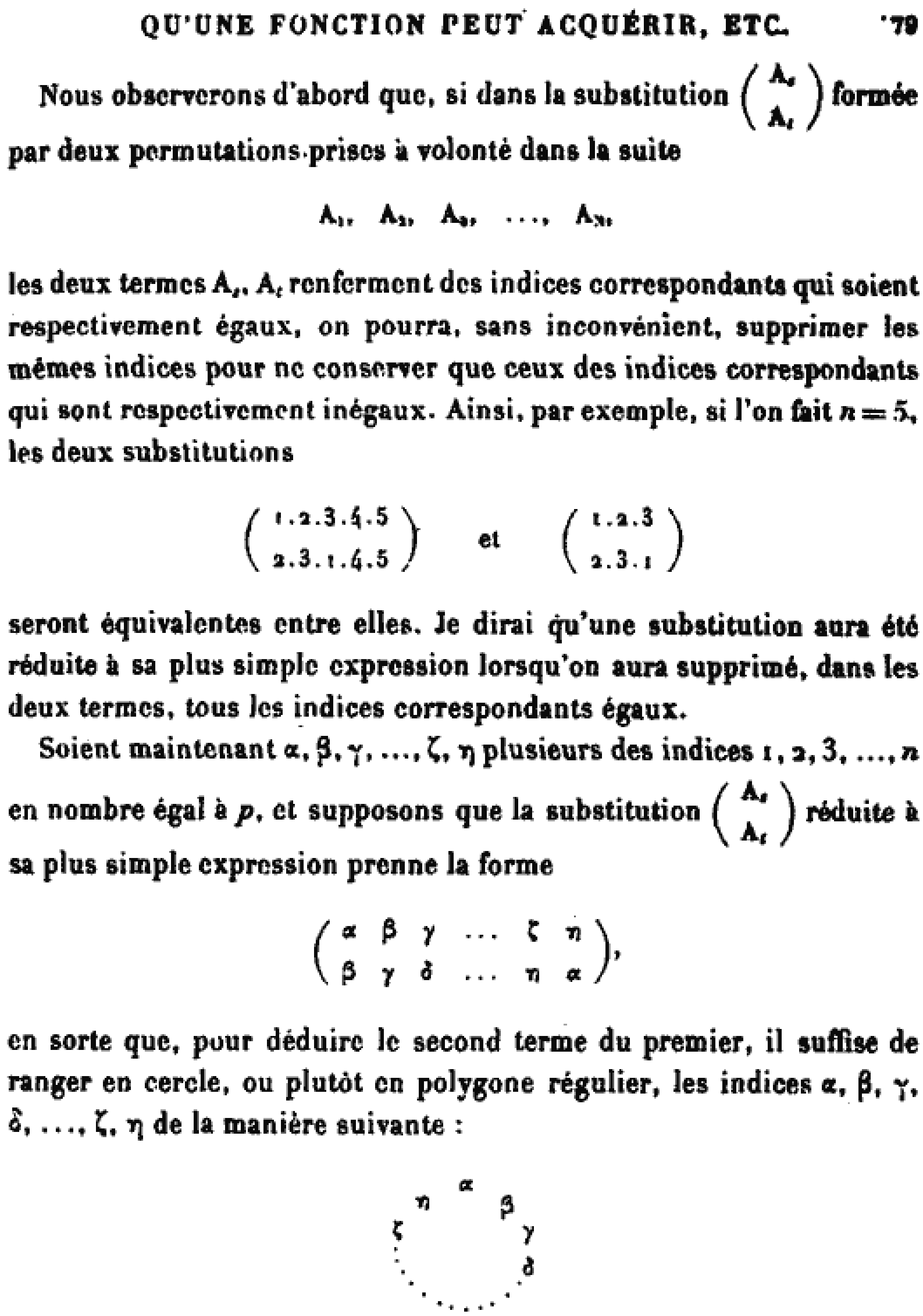


图 2-8 一个循环

图 2-9 是柯西在 1815 年发表的论文的某一页，他介绍了置换的演算．注意到他对循环置换采用的记号是一个圆．



QU'UNE FONCTION PEUT ACQUÉRIR, ETC. 79

Nous observerons d'abord que, si dans la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ formée par deux permutations prises à volonté dans la suite

$$A_1, \ A_2, \ A_3, \ \ldots, \ A_N,$$

les deux termes A_s, A_t renferment des indices correspondants qui soient respectivement égaux, on pourra, sans inconvénient, supprimer les mêmes indices pour ne conserver que ceux des indices correspondants qui sont respectivement inégaux. Ainsi, par exemple, si l'on fait $n = 5$, les deux substitutions

$$\begin{pmatrix} 1.2.3.4.5 \\ 2.3.1.4.5 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1.2.3 \\ 2.3.1 \end{pmatrix}$$

seront équivalentes entre elles. Je dirai qu'une substitution aura été réduite à sa plus simple expression lorsqu'on aura supprimé, dans les deux termes, tous les indices correspondants égaux.

Soient maintenant $\alpha, \beta, \gamma, \ldots, \zeta, \eta$ plusieurs des indices $1, 2, 3, \ldots, n$ en nombre égal à p, et supposons que la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ réduite à sa plus simple expression prenne la forme

$$\begin{pmatrix} \alpha & \beta & \gamma & \ldots & \zeta & \eta \\ \beta & \gamma & \delta & \ldots & \eta & \alpha \end{pmatrix},$$

en sorte que, pour déduire le second terme du premier, il suffise de ranger en cercle, ou plutôt en polygone régulier, les indices α, β, γ, δ, ..., ζ, η de la manière suivante :

α β γ δ ... ζ η

图 2-9 柯西的论文

现在我们给出一个算法，用来把置换分解为一些循环置换的乘积. 例如，取 109~110

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&4&7&2&5&1&8&9&3\end{pmatrix}.$$

从写“(1”开始. 因为 $\alpha: 1\mapsto 6$，所以写“(1 6”. 又因为 $\alpha: 6\mapsto 1$，所以可关闭圆括弧：α 以“(1 6)”开始. 第一个还没有出现的数字是 2，所以我们写“(1 6)(2”. 因为 $\alpha: 2\mapsto 4$，所以写“(1 6)(2 4”. 由于 $\alpha: 4\mapsto 2$，所以又可以关闭圆括弧且我们写“(1 6)(2 4)”. 剩下的最小数是 3，由于 $3\mapsto 7$，$7\mapsto 8$，$8\mapsto 9$，$9\mapsto 3$，这就给出了 4-循环置换(3 7 8 9). 最后 $\alpha(5)=5$. 我们断言

$$\alpha=(1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5).$$

由于 S_n 中的乘法是函数的合成，所以我们的断言是：对 1 到 n 之间的每个 i 有

$$\alpha(i)=[(1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5)](i)$$

(毕竟，两个函数 f，g 相等当且仅当对它们公共定义域中的每个 i 有 $f(i)=g(i)$). 右边是合成 $\beta\gamma\delta$，其中 $\beta=(1\ 6)$，$\gamma=(2\ 4)$，$\delta=(3\ 7\ 8\ 9)$(实际上，也存在 1-循环置换(5)，当我们计算时可以将它忽略，因为(5)是恒等函数). 现在 $\alpha(1)=6$. 置换的乘法是把置换看作函数然后取它们的合成. 例如，若 $i=1$，则

$$\begin{aligned}\beta\gamma\delta(1)&=\beta(\gamma(\delta(1)))\\&=\beta(\gamma(1))\quad\text{因为 }\delta\text{ 固定 }1\\&=\beta(1)\quad\text{因为 }\gamma\text{ 固定 }1\\&=6\end{aligned}$$

在命题 2.24 中，我们将给出 α 可以分解成循环置换的乘积的更令人满意的证明.

把置换分解为循环置换对做置换的乘法是很方便的. 例如，在 S_5 中，让我们通过展示算法的“部分输出成果”来简化乘积

$$\sigma=(1\ 2)(1\ 3\ 4\ 2\ 5)(2\ 5\ 1\ 3)$$

$\sigma: 1\mapsto 3\mapsto 4\mapsto 4$，所以 σ 从(1 4 开始. 然后，$\sigma: 4\mapsto 4\mapsto 2\mapsto 1$，因而 σ 从(1 4)开始. 还没有考虑的最小数是 2，且 $\sigma: 2\mapsto 5\mapsto 1\mapsto 2$，因此 σ 固定 2，σ 从(1 4)(2)开始. 还没有考虑的最小数是 3，且 $\sigma: 3\mapsto 2\mapsto 5\mapsto 5$. 最后，$\sigma: 5\mapsto 1\mapsto 3\mapsto 3$，我们得到

$$\sigma=(1\ 4)(2)(3\ 5).$$

在用上述算法把置换分解为循环置换的过程中，我们注意到，在下述意义下，这些循环置换是不相交的. 111

→ **定义** 两个置换 α，$\beta\in S_n$ 是**不相交的**，若每个 i 被其中一个固定而被另一个移动：若 $\alpha(i)\neq i$，则 $\beta(i)=i$，且若 $\beta(j)\neq j$，则 $\alpha(j)=j$. 一族置换 β_1，…，β_t 是**不相交的**，若每对置换都是不相交的.

考虑循环置换的特殊情形. 若 $\alpha=(i_1 i_2\cdots i_r)$，$\beta=(j_1 j_2\cdots j_s)$，则 $\{i_1, i_2, \cdots, i_r\}\cap\{j_1, j_2, \cdots, j_s\}$ 中的任意 k 既被 α 移动也被 β 移动. 因此，容易看出，两个循环置换不相交当且仅当 $\{i_1, i_2, \cdots, i_r\}\cap\{j_1, j_2, \cdots, j_s\}=\varnothing$，即 $\{i_1, i_2, \cdots, i_r\}$ 和 $\{j_1, j_2, \cdots, j_s\}$ 是不相交的集合.

当置换 α 和 β 不相交时，对数 i 恰有三种不同的可能：被 α 移动，被 β 移动，或既不被 α 移动也不被 β 移动(即被两者都固定).

→ **引理 2.22** 不相交置换 α，$\beta\in S_n$ 是交换的.

证明 只需证明若 $1\leqslant i\leqslant n$，则 $\alpha\beta(i)=\beta\alpha(i)$. 若 β 移动 i，不妨设 $\beta(i)=j\neq i$，则 β 也移动 j[否则，$\beta(j)=j$，$\beta(i)=j$，与 β 是单射矛盾]. 因为 α 和 β 不相交，所以 $\alpha(i)=i$，$\alpha(j)=j$. 因而 $\beta\alpha(i)=j=\alpha\beta(i)$. 类似的讨论可证明若 α 移动 i 则 $\alpha\beta(i)=\beta\alpha(i)$. 最后一种可能是 α 和 β 都不移动 i，此时 $\alpha\beta(i)=i=\beta\alpha(i)$. 因此，由命题 2.2 知，$\alpha\beta=\beta\alpha$. ■

特别地，不相交的循环置换是交换的.

非不相交置换也可能交换. 例如，读者可验证(1 2 3)(4 5)和(1 3 2)(6 7)都是交换的. 一个更简单的例子是，置换和自身交换.

引理 2.23 设 $X=\{1, 2, \cdots, n\}$，$\alpha\in S_X=S_n$，若 $i_1\in X$，则对所有 $j\geqslant 1$ 归纳地定义 i_j：$i_{j+1}=\alpha(i_j)$. 记 $Y=\{i_j : j\geqslant 1\}$，并设 Y' 是 Y 的补集.

(i)若 α 移动 i_1，则存在 $r>1$ 使 i_1，…，i_r 互异，且 $i_{r+1}=\alpha(i_r)=i_1$.

(ii)$\alpha(Y)=Y$，$\alpha(Y')=Y'$.

证明 (i)因为 X 是有限集，所以存在最小的 $r>1$ 使 i_1，…，i_r 互异，但是 $i_{r+1}=\alpha(i_r)\in\{i_1, \cdots, i_r\}$，即对 $1\leqslant j\leqslant r$ 有 $\alpha(i_r)=i_j$. 若 $j>1$，则 $\alpha(i_r)=i_j=\alpha(i_{j-1})$. 但是 α 是一个单射，所以 $i_r=i_{j-1}$，这与 i_1，…，i_r 互异相矛盾. 因此 $\alpha(i_r)=i_1$.

(ii)显然 $\alpha(Y)\subseteq Y$，因为若 $i_j\in Y$，则 $\alpha(i_j)=i_{j+1}\in Y$. 若 $k\in Y'$，则或者 $\alpha(k)\in Y$ 或者 $\alpha(k)\in Y'$，因为 Y' 是 Y 的补集，所以 $X=Y\cup Y'$. 若 $\alpha(k)\in Y$，则对某个 j 有 $\alpha(k)=i_j=\alpha(i_{j-1})$(根据(i)，当 $i_j=i_1$ 时也成立). 因为 α 是单射，所以 $k=i_{j-1}\in Y$，与 $Y\cap Y'=\varnothing$ 矛盾.
112 因此$\alpha(Y')\subseteq Y'$.

我们现在证明 $\alpha(Y)\subseteq Y$ 和 $\alpha(Y')\subseteq Y'$实际上是相同的. 因为 $\alpha(X)=\alpha(Y\cup Y')=\alpha(Y)\cup\alpha(Y')$，它是不相交集合的并，因为 α 是一个单射. 但是由 $\alpha(Y)\subseteq Y$ 得 $|\alpha(Y)|\leqslant|Y|$，由 $\alpha(Y')\subseteq Y'$得 $|\alpha(Y')|\leqslant|Y'|$. 若这些不等式中有严格的，则 $|\alpha(X)|<|X|$. 但是因为 α 是一个满射，所以 $\alpha(X)=X$，矛盾. ■

引理 2.23(i)的证明将会被再次用到.

→ **命题 2.24** 每个置换 $\alpha\in S_n$ 或是一个循环置换，或是不相交循环置换的乘积.

证明 对被 α 移动的点的个数 $k\geqslant 0$ 用归纳法. 基础步骤 $k=0$ 成立，因为此时 α 是恒等函数，即 1-循环置换.

若 $k>0$，则存在被 α 移动的点，不妨设为 i_1. 和在引理 2.23 中一样，定义 $Y=\{i_1, i_2, \cdots, i_r\}$，其中 i_1，i_2，…，i_r 是互异的，对 $j<r$，$\alpha(i_j)=i_{j+1}$，且 $\alpha(i_r)=i_1$. 设 $\sigma\in S_X$ 是 r-循环 $(i_1 i_2 i_3\cdots i_r)$，所以 σ 固定 Y 的补集 Y'中的每一点，如果还有的话. 若 $r=n$，则 $\alpha=\sigma$. 若 $r<n$，则 $\alpha(Y')=Y'$，和在引理中一样. 定义 $\alpha'=\alpha\sigma^{-1}$，我们断言 α'和 σ 不相交. 若 σ 移动 i，则 $i=i_j\in Y$. 但是 $\alpha'(i_j)=\alpha\sigma^{-1}(i_j)=\alpha(i_{j-1})=i_j$，即 α'固定 i_j. 假设 α'移动某一点 i'，我们刚才已经看到 $i'\notin Y$，所以可以假设 $i'\in Y'$. 根据定义，σ 固定 Y' 中的每一点，因而 σ 固定 i'. 因此，$\alpha=\alpha'\sigma$是两个不相交置换的积. 被 α'移动的点的个数是 $k-r<k$，所以由归纳假设知 $\alpha'=\beta_1\cdots\beta_t$，

其中 β_1，…，β_t 是不相交的循环置换. 因此 $\alpha=\alpha'\sigma=\beta_1\cdots\beta_t\sigma$ 是不相交循环置换的积，证毕. ■

我们已经证明了前面介绍的算法的输出结果总是不相交循环置换的积.

通常我们在这种分解中会隐去 1-循环置换[因为 1-循环置换等于恒等函数(1)]. 但是，α 的含有关于被 α 固定的 i 的 1-循环置换的分解将在后面的内容中出现.

→ **定义** 置换 α 的一个**完全分解**是指：将 α 分解成不相交循环置换的乘积且含有关于被 α 固定的每个 i 的 1-循环置换 (i).

分解算法总会产生完全分解. 例如，若

$$\alpha=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 2 & 5\end{pmatrix},$$

则由算法得 $\alpha=(1)(2\ 3\ 4)(5)$，是一个完全分解. 但是，若我们隐去 1-循环置换，则分解

$$\alpha=(2\ 3\ 4)=(1)(2\ 3\ 4)=(2\ 3\ 4)(5)$$ 113

不是完全分解. 在一个完全分解 $\alpha=\beta_1\cdots\beta_t$ 中，1 和 n 之间的每个符号 i 在这些 β 中恰出现一次.

若 $\beta\in S_n$，$k\geqslant 0$，则归纳地定义 β 的**幂**：$\beta^0=(1)$，$\beta^{k+1}=\beta\beta^k$. 因此，β^k 是 β 和自身的 k 次合成. r-循环置换 β 和它的幂之间存在着关系. 我们稍微改变一下符号，记 $\beta=(i_0 i_1\cdots i_{r-1})$. 注意 $i_1=\beta(i_0)$，$i_2=\beta(i_1)=\beta(\beta(i_0))=\beta^2(i_0)$，$i_3=\beta(i_2)=\beta(\beta^2(i_0))=\beta^3(i_0)$，且对所有 $k\leqslant r-1$，

$$i_k=\beta^k(i_0). \tag{1}$$

由于 $\beta(i_{r-1})=i_0$，容易看出：当符号 i_j 中的 j 是取自模 r 的数时，式子 $i_k=\beta^k(i_0)$ 成立.

引理 2.25 (i)设 $\alpha=\beta\delta$ 是不相交循环置换的积，若 β 移动 i，则对所有 $k\geqslant 1$，$\alpha^k(i)=\beta^k(i)$.

(ii)若 β 和 γ 都是移动 $i=i_0$ 的循环置换，且对所有 $k\geqslant 1$ 有 $\beta^k(i)=\gamma^k(i)$，则 $\beta=\gamma$.

注 (ii)中的前提条件不是假设循环置换 β 和 γ 有相同的长度，但这是结论的一部分.

证明 (i)由于 β 移动 i，所以由不相交知 δ 固定 i. 事实上，δ 的每个幂固定 i. 根据引理 2.22，β 和 δ 交换，所以由习题 2.30(i)知 $(\beta\delta)^k(i)=\beta^k(\delta^k(i))=\beta^k(i)$，证毕.

(ii)根据式子(1)，若 $\beta=(i_0 i_1\cdots i_{r-1})$，则对所有 $k<r-1$ 有 $i_k=\beta^k(i_0)$. 类似地，若 $\gamma=(i_0 j_1\cdots j_{s-1})$，则对 $k<s-1$ 有 $j_k=\gamma^k(i_0)$. 我们可假设 $r\leqslant s$ 使得 $i_1=j_1$，…，$i_{r-1}=j_{r-1}$. 因为 $j_r=\gamma^r(i_0)=\beta^r(i_0)=i_0$，所以 $s-1=r-1$，且对所有 k 有 $j_k=i_k$，所以 $\beta=(i_0 i_1\cdots i_{r-1})=\gamma$. ■

下述定理是算术基本定理的一个类似结论.

→ **定理 2.26** 设 $\alpha\in S_n$，$\alpha=\beta_1\cdots\beta_t$ 是一个完全分解. 若不考虑循环置换出现的顺序，则这个分解是唯一的.

证明 设 $\alpha=\gamma_1\cdots\gamma_s$ 是 α 的另一个完全分解. 因为 α 的每个完全分解恰有一个关于被 α 固定的每个 i 的 1-循环置换，所以只需对 t 和 s 的较大者 ℓ 归纳地证明长度 >1 的循环置换由 α 唯一确定.

基础步骤是成立的，因为当 $\ell=1$ 时，前提条件即为 $\beta_1=\alpha=\gamma_1$. 114

为证明归纳步骤，首先注意到，若 β_t 移动 $i=i_0$，则由引理 2.25(i)知，对所有 $k\geqslant 1$ 有 $\beta_t^k(i_0)=\alpha^k(i_0)$. 现在某个 γ_j 一定会移动 i_0. 因为不相交循环置换交换，所以我们可重给下标使

得 γ_s 移动 i_0. 如前所述，对所有 k 有 $\gamma_s^k(i_0)=\alpha^k(i_0)$. 于是由引理 2.25(ii)知 $\beta_t=\gamma_s$，且由消去律得 $\beta_1\cdots\beta_{t-1}=\gamma_1\cdots\gamma_{s-1}$. 根据归纳假设得 $s=t$，且这些 γ 可重给下标使得 $\gamma_1=\beta_1$，…，$\gamma_{t-1}=\beta_{t-1}$.

■

每个置换都是一个双射，那么我们怎样找到一个置换的逆？在图 2-8 中，循环置换 β 被形象地描述成圆周的顺时针旋转，其逆 β^{-1} 恰是反时针旋转.

命题 2.27

(i)循环置换 $\alpha=(i_1 i_2\cdots i_r)$ 的逆是 $(i_r i_{r-1}\cdots i_1)$：

$$(i_1 i_2\cdots i_r)^{-1}=(i_r i_{r-1}\cdots i_1).$$

(ii)若 $\gamma\in S_n$ 且 $\gamma=\beta_1\cdots\beta_k$，则

$$\gamma^{-1}=\beta_k^{-1}\cdots\beta_1^{-1}$$

(注意 γ^{-1} 中因子的顺序被颠倒过来了).

证明 (i)若 $\alpha\in S_n$，我们证明这两个循环置换的合成等于(1). 现在 $(i_1 i_2\cdots i_r)(i_r i_{r-1}\cdots i_1)$ 固定 1 与 n 之间不同于 i_1，$\cdots i_r$ 的每个整数(如果还有的话). 当这个合成对 $i_j(j\geqslant 2)$ 作用时有 $i_j\mapsto i_{j-1}\mapsto i_j$，并且 $i_1\mapsto i_r\mapsto i_1$. 因此 1 与 n 之间的每个整数都被这个合成固定，所以它是(1). 类似的讨论可证明另一顺序的合成也等于(1)，于是

$$(i_1 i_2\cdots i_r)^{-1}=(i_r i_{r-1}\cdots i_1).$$

(ii)对 $k\geqslant 2$ 应用归纳法. 对基础步骤 $k=2$，我们有

$$(\beta_1\beta_2)(\beta_2^{-1}\beta_1^{-1})=\beta_1(\beta_2\beta_2^{-1})\beta_1^{-1}=\beta_1\beta_1^{-1}=(1).$$

类似地，$(\beta_2^{-1}\beta_1^{-1})(\beta_1\beta_2)=(1)$.

对归纳步骤，设 $\delta=\beta_1\cdots\beta_k$，使得 $\beta_1\cdots\beta_k\beta_{k+1}=\delta\beta_{k+1}$. 则

$$\begin{aligned}(\beta_1\cdots\beta_k\beta_{k+1})^{-1}&=(\delta\beta_{k+1})^{-1}\\&=\beta_{k+1}^{-1}\delta^{-1}\\&=\beta_{k+1}^{-1}(\beta_1\cdots\beta_k)^{-1}\\&=\beta_{k+1}^{-1}\beta_k^{-1}\cdots\beta_1^{-1}.\end{aligned}$$

■

因此，$(1\ 2\ 3\ 4)^{-1}=(4\ 3\ 2\ 1)=(1\ 4\ 3\ 2)$，$(1\ 2)^{-1}=(2\ 1)=(1\ 2)$(每个对换都等于自己
115 的逆).

例 2.28 特别地，若因子是不相交的循环置换，则命题 2.27 中的结果也成立(此时，根据引理 2.22，因子顺序的颠倒是没有必要的，因为它们交换). 因此，若

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&4&7&2&5&1&8&9&3\end{pmatrix},$$

则 $\alpha=(1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5)$ 且

$$\begin{aligned}\alpha^{-1}&=(5)(9\ 8\ 7\ 3)(4\ 2)(6\ 1)\\&=(1\ 6)(2\ 4)(3\ 9\ 8\ 7).\end{aligned}$$

◀

→ **定义** 称两个置换 α，$\beta\in S_n$ 有**相同的循环结构**，如果在它们的完全分解中每个 r-循环置换的数目都相同($r\geqslant 1$).

根据习题 2.24，S_n 中存在

$$(1/r)[n(n-1)\cdots(n-r+1)]$$

个 r-循环置换．如果某种置换分解为几个相同长度的循环置换的积，则我们可以用这个公式来计算这种置换的个数．例如，S_4 中形如 $(a\ b)(c\ d)$ 的置换的个数是

$$\frac{1}{2}\left[\frac{1}{2}(4\times 3)\right]\times\left[\frac{1}{2}(2\times 1)\right]=3,$$

外面因子 $\frac{1}{2}$ 的出现是指我们不能对 $(a\ b)(c\ d)=(c\ d)(a\ b)$ 计算两次．类似地，S_n 中形如 $(a\ b)(c\ d)(e\ f)$ 的置换的个数是

$$\frac{1}{3!2^3}[n(n-1)(n-2)(n-3)(n-4)(n-5)]$$

（见习题 2.24）．

例 2.29

表 2-1　S_4 中的置换

循环结构	个数
(1)	1
(1 2)	6
(1 2 3)	8
(1 2 3 4)	6
(1 2)(3 4)	3
	24

◀

例 2.30

表 2-2　S_5 中的置换

循环结构	个数
(1)	1
(1 2)	10
(1 2 3)	20
(1 2 3 4)	30
(1 2 3 4 5)	24
(1 2)(3 4 5)	20
(1 2)(3 4)	15
	120

◀ 116

引理 2.31　设 α，$\gamma\in S_n$．对所有 i，若 $\gamma: i\mapsto j$，则 $\alpha\gamma\alpha^{-1}: \alpha(i)\mapsto\alpha(j)$．

证明

$$\alpha\gamma\alpha^{-1}(\alpha(i))=\alpha\gamma(i)=\alpha(j).$$ ■

命题 2.32　设 γ，$\alpha\in S_n$，则 $\alpha\gamma\alpha^{-1}$ 和 γ 有相同的循环结构．更详细地说，若 γ 的完全分解是

$$\gamma=\beta_1\beta_2\cdots(i\ j\cdots)\cdots\beta_t,$$

则 $\alpha\gamma\alpha^{-1}$ 是用 α 作用 γ 的循环置换中的符号而得到的一个置换 σ．

注　例如，若 $\gamma=(1\ 3)(2\ 4\ 7)(5)(6)$，$\alpha=(2\ 5\ 6)(1\ 4\ 3)$，则

$$\alpha\gamma\alpha^{-1}=(\alpha 1\ \alpha 3)(\alpha 2\ \alpha 4\ \alpha 7)(\alpha 5)(\alpha 6)=(4\ 1)(5\ 3\ 7)(6)(2).$$

证明　若 γ 固定 i，则引理 2.31 表明 σ 固定 $\alpha(i)$．假设 γ 移动一个符号 i，不妨设 $\gamma(i)=j$，则在 γ 的完全分解中一个循环置换是

$$(i\ j\cdots).$$

根据 σ 的定义，它的一个循环置换为

$$(\alpha(i)\ \alpha(j)\ \cdots),$$

即 $\sigma: \alpha(i) \mapsto \alpha(j)$. 但是引理 2.31 是说 $\alpha\gamma\alpha^{-1}: \alpha(i) \mapsto \alpha(j)$，所以 σ 和 $\alpha\gamma\alpha^{-1}$ 对形如 $\alpha(i)$ 的所
117 有符号一致. 但是因为 $\alpha: X \to X$ 是一个满射，每个 $k \in X$ 有形式 $k = \alpha(i)$，所以 $\sigma = \alpha\gamma\alpha^{-1}$. ■

→ **命题 2.33** *若 $\gamma, \gamma' \in S_n$，则 γ 和 γ' 有相同的循环结构当且仅当存在 $\alpha \in S_n$ 使 $\gamma' = \alpha\gamma\alpha^{-1}$.*

证明 充分性刚才在命题 2.32 中已经证明.

反过来，假设 γ 和 γ' 有相同的循环结构，即 $\gamma = \beta_1 \cdots \beta_t$ 和 $\gamma' = \sigma_1 \cdots \sigma_t$ 都是完全分解，其中对所有 $\lambda \leqslant t$，β_λ 和 σ_λ 有相同的长度. 设 $\beta_\lambda = (i_1^\lambda, \cdots, i_{r(\lambda)}^\lambda)$，$\sigma_\lambda = (j_1^\lambda, \cdots, j_{r(\lambda)}^\lambda)$. 对所有 λ 定义

$$\alpha(i_1^\lambda) = j_1^\lambda, \alpha(i_2^\lambda) = j_2^\lambda, \cdots, \alpha(i_{r(\lambda)}^\lambda) = j_{r(\lambda)}^\lambda.$$

因为 $\beta_1 \cdots \beta_t$ 是一个完全分解，所以每个 $i \in X = \{1, \cdots, n\}$ 只在一个 β_λ 中出现，因而 $\alpha(i)$ 对每个 $i \in X$ 有定义，且 $\alpha: X \to X$ 是一个(单值)函数. 因为 $\sigma_1 \cdots \sigma_t$ 是一个完全分解，所以每个 $j \in X$ 在某个 σ_λ 中出现，于是 α 是满的. 根据习题 2.13，α 是一个双射，且 $\alpha \in S_n$. 命题 2.32 是说 $\alpha\gamma\alpha^{-1}$ 和 γ 有相同的循环结构，且对每个 λ，第 λ 个循环置换是

$$(\alpha(i_1^\lambda)\alpha(i_2^\lambda)\cdots\alpha(i_{r(\lambda)}^\lambda)) = \sigma_\lambda.$$

因此 $\alpha\gamma\alpha^{-1} = \gamma'$. ■

例 2.34 若

$$\gamma = (1\ 2\ 3)(4\ 5)(6), \quad \gamma' = (2\ 5\ 6)(3\ 1)(4),$$

则 $\gamma' = \alpha\gamma\alpha^{-1}$，其中

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 5)(3\ 6\ 4).$$

注意 α 还有其他的选择. ◀

置换还有另一种有用的分解.

→ **命题 2.35** *若 $n \geqslant 2$，则每个 $\alpha \in S_n$ 是一些对换的乘积.*

证明 根据命题 2.24，只需将一个 r-循环置换 β 分解成一些对换的乘积. 方法如下. 若 $r = 1$，则 β 是恒等函数，且 $\beta = (1\ 2)(1\ 2)$. 若 $r \geqslant 2$，则

$$\beta = (1\ 2\ \cdots\ r) = (1\ r)(1\ r-1)\cdots(1\ 3)(1\ 2).$$

[我们可通过计算每一边来检验这是一个等式. 例如，左边 $\beta: 1 \mapsto 2$；因为 $(1\ r)$，$(1\ r-1)$，…，
118 $(1\ 3)$ 中每一个都固定 2，所以右边也是 $1 \mapsto 2$.] ■

因此每个置换可被当作是一系列的对换. 这样的分解没有分解成不相交循环置换的乘积好. 首先，对换不要求交换：$(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$. 其次，不论是因子本身还是因子的次序都不能被唯一确定. 例如，以下是 S_4 中 $(1\ 2\ 3)$ 的一些分解：

$$\begin{aligned}(1\ 2\ 3) &= (1\ 3)(1\ 2) \\ &= (2\ 3)(1\ 3) \\ &= (1\ 3)(4\ 2)(1\ 2)(1\ 4) \\ &= (1\ 3)(4\ 2)(1\ 2)(1\ 4)(2\ 3)(2\ 3).\end{aligned}$$

这样的分解究竟有没有唯一性呢？我们现在证明：在置换 α 的所有这样的分解中，因子个数的奇偶性是相同的，即对换的个数总是偶数个或者总是奇数个[正如上述 $\alpha = (1\ 2\ 3)$ 的分解所暗

示的一样].

例 2.36 15-字谜由一个**起始位置**构成，它是由 1 与 15 之间的数字和一个符号 #(我们把这个符号翻译成"空白")构成的 4×4 列阵，还包括简单的移动. 例如，考虑下面给出的起始位置.

3	15	4	12
10	11	1	8
2	5	13	9
6	7	14	#

一个**简单移动**是指用一个与空白接近的符号来与空白交换. 例如，上面的起始位置存在两个开始的简单移动：或者交换 # 和 14，或者交换 # 和 9. 在一系列简单移动之后，如果起始位置被改变为标准列阵 1，2，3，…，15，#，那么我们就赢了这个游戏.

为了分析这个游戏，注意到给定的列阵实际上是一个置换 $\alpha \in S_{16}$. 准确地说，α 置换{1，2，…，15，#}：若这些方格标上 1 到 15 之间的数字和 #，则设 $\alpha(i)$ 是占在第 i 个方格中的符号. 例如，上面给定的起始位置是

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \# \\ 3 & 15 & 4 & 12 & 10 & 11 & 1 & 8 & 2 & 5 & 13 & 9 & 6 & 7 & 14 & \# \end{pmatrix}.$$

每个简单移动是一个特殊的对换，即移动 # 的对换. 另外，对一个位置(对应于一个置换 β)实施一个简单移动(对应于一个特殊对换 τ)，结果产生一个对应于置换 $\tau\beta$ 的新的位置. 例如，若 α 是上面的位置，τ 是交换 14 和 # 的对换，则 $\tau\alpha(\#)=\tau(\#)=14$，且 $\tau\alpha(15)=\tau(14)=\#$，而 119
对所有其他 i 有 $\tau\alpha(i)=i$. 也就是说，新的构造有原先位置中的所有数字，除了 14 和 # 被交换之外. 因此，为了赢得这个游戏，我们需要一些特殊的对换 τ_1，τ_2，…，τ_m 使得

$$\tau_m \cdots \tau_2 \tau_1 \alpha = (1).$$

这表明在赢得这个游戏的过程中 α 的选择有几种，但是正如我们将在例 2.42 中看到的一样，α 的其他选择都会导致游戏失败. ◀

下面的讨论将使我们能够进一步分析 15-游戏.

引理 2.37 *若 k，$\ell \geqslant 0$，且字母 a，b，c_i，d_j 是互不相同的，则*

$$(a\,b)(a\,c_1 \cdots c_k\,b\,d_1 \cdots d_\ell) = (a\,c_1 \cdots c_k)(b\,d_1 \cdots d_\ell)$$

和

$$(a\,b)(a\,c_1 \cdots c_k)(b\,d_1 \cdots d_\ell) = (a\,c_1 \cdots c_k\,b\,d_1 \cdots d_\ell).$$

证明 第一个要证明的等式左边有

$$\begin{aligned} a &\mapsto c_1 \mapsto c_1; \\ c_i &\mapsto c_{i+1} \mapsto c_{i+1}, \quad \text{当 } i < k \text{ 时}; \\ c_k &\mapsto b \mapsto a; \\ b &\mapsto d_1 \mapsto d_1; \\ d_j &\mapsto d_{j+1} \mapsto d_{j+1}, \quad \text{当 } j < \ell \text{ 时}; \\ d_\ell &\mapsto a \mapsto b. \end{aligned}$$

对右边作类似的计算，可知两个置换对 a，b 和所有 c_i，d_j 一致. 由于每边都固定{1，2，…，n}中的其他数(如果还有的话)，所以两边相等.

关于第二个等式，把第一个等式倒过来有

$$(a\,c_1\cdots c_k)(b\,d_1\cdots d_\ell)=(a\,b)(a\,c_1\cdots c_k\,b\,d_1\cdots d_\ell),$$

只要在两边左乘$(a\,b)$即可得：

$$(a\,b)(a\,c_1\cdots c_k)(b\,d_1\cdots d_\ell)=(a\,b)(a\,b)(a\,c_1\cdots c_k\,b\,d_1\cdots d_\ell)$$
$$=(a\,c_1\cdots c_k\,b\,d_1\cdots d_\ell)$$ ■

引理的一个例子是

120 $$(1\ 2)(1\ 3\ 4\ 2\ 5\ 6\ 7)=(1\ 3\ 4)(2\ 5\ 6\ 7).$$

→ **定义** 设$\alpha\in S_n$且$\alpha=\beta_1\cdots\beta_t$是完全分解，则符号[⊖]$\alpha$定义为

$$\mathrm{sgn}(\alpha)=(-1)^{n-t}.$$

定理 2.26 表明 sgn 是一个(单值)函数，因为循环置换的个数t被α唯一确定．若ε是一个1-循环置换，则$\mathrm{sgn}(\varepsilon)=1$，因为$t=n$且$\mathrm{sgn}(\varepsilon)=(-1)^0=1$．若$\tau$是一个对换，则它移动两个数，并固定其他$n-2$个数．因此，$t=1+(n-2)=n-1$，所以$\mathrm{sgn}(\tau)=(-1)^{n-(n-1)}=-1$.

引理 2.38 若α，$\tau\in S_n$，其中τ是一个对换，则

$$\mathrm{sgn}(\tau\alpha)=-\mathrm{sgn}(\alpha).$$

证明 设$\alpha=\beta_1\cdots\beta_t$是$\alpha$的完全分解，并设$\tau=(ab)$．若$a$和$b$出现在同一个$\beta$中，不妨设同出现在$\beta_1$中，则$\beta_1=(a\,c_1\cdots c_k\,b\,d_1\cdots d_\ell)$，其中$k$，$\ell\geqslant 0$．根据引理 2.37，

$$\tau\beta_1=(a\,c_1\cdots c_k)(b\,d_1\cdots d_\ell).$$

这是$\tau\alpha=(\tau\beta_1)\beta_2\cdots\beta_t$的完全分解，因为其中的循环置换是两两不相交的且$\{1,2,\cdots,n\}$中的每个数只在一个循环置换中出现．因此，$\tau\beta$有$t+1$个循环置换，这是因为$\tau\beta_1$分解成了两个不相交循环置换．因此$\mathrm{sgn}(\tau\alpha)=(-1)^{n-(t+1)}=-\mathrm{sgn}(\alpha)$.

另一个可能是a和b出现在不同的循环置换中，不妨设$\beta_1=(a\,c_1\cdots c_k)$，$\beta_2=(b\,d_1\cdots d_\ell)$，其中$k$，$\ell\geqslant 0$．但是$\tau\alpha=(\tau\beta_1\beta_2)\beta_3\cdots\beta_t$，由引理 2.37 得

$$\tau\beta_1\beta_2=(a\,c_1\cdots c_k\,b\,d_1\cdots d_\ell).$$

因此$\mathrm{sgn}(\tau\alpha)=(-1)^{n-(t-1)}=-\mathrm{sgn}(\alpha)$，这是因为在$\tau\alpha$的完全分解中有$t-1$个循环置换． ■

→ **定理 2.39** 对所有α，$\beta\in S_n$，

$$\mathrm{sgn}(\alpha\beta)=\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).$$

证明 假设给定$\alpha\in S_n$，α可分解成m个对换的积：$\alpha=\tau_1\cdots\tau_m$．我们对$m$应用归纳法证
121 明：对每个$\beta\in S_n$有$\mathrm{sgn}(\alpha\beta)=\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$．基础步骤$m=1$就是引理 2.38，因为$m=1$是说$\alpha$是一个对换．若$m>1$，则对$\tau_2\cdots\tau_m$应用归纳假设得

$$\begin{aligned}\mathrm{sgn}(\alpha\beta)&=\mathrm{sgn}(\tau_1\cdots\tau_m\beta)\\&=-\mathrm{sgn}(\tau_2\cdots\tau_m\beta)&&\text{(引理 2.38)}\\&=-\mathrm{sgn}(\tau_2\cdots\tau_m)\mathrm{sgn}(\beta)&&\text{(归纳假设)}\\&=\mathrm{sgn}(\tau_1\cdots\tau_m)\mathrm{sgn}(\beta)&&\text{(引理 2.38)}\\&=\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).\end{aligned}$$ ■

对$k\geqslant 2$应用归纳法得

⊖ “符号(Signum)”是“记号(mark)”或“记号(token)”的拉丁词，当然它后来演变成了单词“符号(sign)”.

$$\operatorname{sgn}(\alpha_1\alpha_2\cdots\alpha_k) = \operatorname{sgn}(\alpha_1)\operatorname{sgn}(\alpha_2)\cdots\operatorname{sgn}(\alpha_k).$$

→ **定义** 称置换 $\alpha\in S_n$ 为**偶置换**，若 $\operatorname{sgn}(\alpha)=1$；称 α 为**奇置换**，若 $\operatorname{sgn}(\alpha)=-1$. 我们说 α 和 β **同奇偶性**，若它们都是偶置换或都是奇置换.

我们回到置换分解成一些对换的积上来. 前面我们看到，一个置换有很多种这样的分解，这些不同分解的唯一共同点是因子的数目同奇偶性. 为证明这一点，我们必须证明，一个置换不可能既是偶数个对换的积又是奇数个对换的积.

→ **定理 2.40** (i)设 $\alpha\in S_n$. 若 α 是偶置换，则 α 是偶数个对换的积；若 α 是奇置换，则 α 是奇数个对换的积.

(ii)若 $\alpha=\tau_1\cdots\tau_q=\tau_1'\cdots\tau_p'$ 是一些对换的积，则 q 和 p 同奇偶性.

证明 (i)若 $\alpha=\tau_1\cdots\tau_q$ 是一些对换的积，则由定理 2.39 知，$\operatorname{sgn}(\alpha)=\operatorname{sgn}(\tau_1)\cdots\operatorname{sgn}(\tau_q)=(-1)^q$，这是因为每个对换是奇置换. 因此，若 α 是偶置换，即若 $\operatorname{sgn}(\alpha)=1$，则 q 是偶数，而若 α 是奇置换，即若 $\operatorname{sgn}(\alpha)=-1$，则 q 是奇数.

(ii)假设 α 的分解有两个，一个是奇数个对换的积，另一个是偶数个对换的积，则 $\operatorname{sgn}(\alpha)$ 会有两个不同的值，所以假设不成立. ■

推论 2.41 设 α，$\beta\in S_n$. 若 α 和 β 同奇偶性，则 $\alpha\beta$ 是偶置换；而若 α 和 β 奇偶性不同，则 $\alpha\beta$ 是奇置换. 122

证明 若 $\operatorname{sgn}(\alpha)=(-1)^q$，$\operatorname{sgn}(\beta)=(-1)^p$，则由定理 2.39 知，$\operatorname{sgn}(\alpha\beta)=(-1)^{q+p}$，由此得到结论. ■

例 2.42 在例 2.36 中对 15-字谜的进一步分析表明，若 $\alpha\in S_{16}$ 是起始位置，则游戏可以赢当且仅当 α 是一个固定 # 的偶置换. 关于这个事实的证明，请读者看麦科伊(McCoy)和贾努兹(Janusz)编写的《近世代数导引》(Introduction to Modern Algebra). 但是在一个方向上的证明是很清楚的. 空格 # 在位置 16 处开始. 每个简单的移动都把 # 向上、向下、向左或向右移动. 因此移动的总次数 m 是 $u+d+l+r$，其中 u 是向上移动的次数，等等. 若 # 被移动到原来的位置，则这些移动都是徒劳的：一定有相同个数的上移和下移，即 $u=d$，且左移和右移的个数相等，即 $r=l$. 因此移动的总次数是偶数：$m=2u+2r$. 即若 $\tau_m\cdots\tau_1\alpha=(1)$，则 m 是偶数，因而 $\alpha=\tau_1\cdots\tau_m$(因为对每个对换 τ 有 $\tau^{-1}=\tau$)，所以 α 是一个偶置换. 有了这个定理，我们检查例 2.36 中的起始位置 α 的完全分解：

$$\alpha = (1\ 3\ 4\ 12\ 9\ 2\ 15\ 14\ 7)(5\ 10)(6\ 11\ 13)(8)(\#),$$

其中(8)和(#)是 1-循环置换. 现在 $\operatorname{sgn}(\alpha)=(-1)^{16-5}=-1$，所以 α 是一个奇置换，因此游戏若从 α 开始则不能赢. ◀

习题

H 2.21 判断对错并说明理由.

(i) n 次对称群是由 n 个元素构成的集合.

(ii)若 $\sigma\in S_6$，则对某个 $n\geq 1$ 有 $\sigma^n=1$.

(iii)若 α，$\beta\in S_n$，则 $\alpha\beta$ 是 $\alpha\circ\beta$ 的缩写.

(iv)若 α，β 都是 S_n 中的循环置换，则 $\alpha\beta=\beta\alpha$.

(v)若 σ，τ 都是 S_n 中的 r-循环置换，则 $\sigma\tau$ 是一个 r-循环置换.

(vi)若 $\sigma\in S_n$ 是一个 r-循环置换，则对每个 $\alpha\in S_n$，$\alpha\sigma\alpha^{-1}$是一个 r-循环置换.

(vii)每个对换都是一个偶置换.

(viii)若置换 α 是 3 个对换的积，则它不能是 4 个对换的积.

(ix)若置换 α 是 3 个对换的积，则它不能是 5 个对换的积.

(x)若 $\sigma\alpha\sigma^{-1}=\omega\alpha\omega^{-1}$，则 $\sigma=\omega$.

*2.22 求出 $\mathrm{sgn}(\alpha)$和 α^{-1}，其中

123

$$\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&8&7&6&5&4&3&2&1\end{pmatrix}.$$

H 2.23 设 $\sigma\in S_n$ 固定某个 j，其中 $1\leqslant j\leqslant n$(即 $\sigma(j)=j$)，定义 $\sigma'\in S_X$，其中 $X=\{1,\cdots,\hat{j},\cdots,n\}$，对所有 $i\neq j$有 $\sigma'(i)=\sigma(i)$. 证明

$$\mathrm{sgn}(\sigma')=\mathrm{sgn}(\sigma).$$

*2.24 H (i)若 $1<r\leqslant n$，证明在 S_n 中存在

$$\frac{1}{r}[n(n-1)\cdots(n-r+1)]$$

个 r-循环置换.

(ii)若 $kr\leqslant n$，其中 $1<r\leqslant n$，证明置换 $\alpha\in S_n$ 的个数是

$$\frac{1}{k!}\frac{1}{r^k}[n(n-1)\cdots(n-kr+1)],$$

其中 α 是 k 个不相交 r-循环置换的积.

*2.25 H (i)若 α 是一个 r-循环置换，证明 $\alpha^r=(1)$.

H (ii)若 α 是一个 r-循环置换，证明 r 是使得 $\alpha^k=(1)$成立的最小正整数 k.

2.26 证明一个 r-循环置换是偶置换当且仅当 r 是奇数.

H 2.27 给定 $X=\{1,2,\cdots,n\}$，我们称 X 的一个置换 τ 是一个邻接，若它是形如$(i\ i+1)$的对换，其中 $i<n$. 若 $i<j$，证明$(i\ j)$是奇数个邻接的积.

*2.28 定义 f：$\{0,1,2,\cdots,10\}\to\{0,1,2,\cdots,10\}$为

$$f(n)=4n^2-3n^7\text{ 被 11 除后的余数.}$$

(i)证明 f 是一个置换.

(ii)计算 f 的奇偶性.

(iii)计算 f 的逆.

2.29 H (i)置换 $\alpha\in S_n$ 是正则置换，若 α 没有固定点且是相同长度的不相交循环置换的积，或者 $\alpha=(1)$. 证明，α 是正则置换当且仅当 α 是一个 n-循环置换的幂.

(ii)证明，若 α 是一个 r-循环置换，则 α^k 是(r,k)个不相交循环置换的积，且每个循环置换的长度为 $r/(r,k)$.

(iii)若 p 是一个素数，证明 p-循环置换的任何幂都是 p-循环置换或(1).

(iv)S_5 中有多少个正则置换？S_8 中有多少个正则置换？

*2.30 H (i)证明，若 α 和 β 都是置换(不一定不相交)且交换，则对所有 $k\geqslant 1$ 有$(\alpha\beta)^k=\alpha^k\beta^k$.

(ii)给出满足$(\alpha\beta)^2\neq\alpha^2\beta^2$的两个置换 α 和 β 的例子.

*2.31 (i)证明，对所有 i，$\alpha\in S_n$ 移动 i 当且仅当 α^{-1}移动 i.

(ii)证明，若 $\alpha,\beta\in S_n$ 是不相交的，且 $\alpha\beta=(1)$，则 $\alpha=(1)$，$\beta=(1)$.

*H 2.32 若 $n\geq 2$，证明 S_n 中偶置换的个数是 $\frac{1}{2}n!$.

2.33 给出 $\alpha, \beta, \gamma \in S_5$ 的例子，其中任何一个都不是(1)，并满足 $\alpha\beta=\beta\alpha$ 和 $\alpha\gamma=\gamma\alpha$，但 $\beta\gamma\neq\gamma\beta$.

*2.34 若 $n\geq 3$，证明，若 $\alpha\in S_n$ 和每个 $\beta\in S_n$ 交换，则 $\alpha=(1)$. 124

H 2.35 右侧的 15-字谜能赢吗?

4	10	9	1
8	2	15	6
12	5	11	3
7	14	13	#

→2.3 群

早在 1500 年，数学家们就推广了二次公式来求解二次、三次多项式的根. 在随后的三个世纪里，许多数学家努力探索类似的公式来求解高次多项式的根. 但是在 1824 年，阿贝尔(N. H. Abel，1802—1829)证明了一般的五次多项式不能用公式求根. 1831 年，伽罗瓦(E. Galois，1811—1832)找到了任意次数的多项式能用公式求根的一般判别方法，从而完全解决了这个问题. 他的基本思想包含了群的思想. 从伽罗瓦时代起，群出现在数学的许多领域，因为群也是描述对称概念的一种方式，我们将在本节的后面部分以及第 6 章看到这一点.

“积”的本质是指：两个事物被结合为第三个同种事物. 例如，普通乘法、加法和减法把两个数结合为第三个数，而合成把两个置换结合为第三个置换.

→ **定义** *集合 G 上的(二元)* **运算** *是指函数*

$$*: G\times G\to G.$$

详细地说，一个运算分派 G 中的元素 $*(x, y)$ 给 G 中元素的有序对 (x, y). 用 $x*y$ 代替 $*(x, y)$ 显得更自然. 这样，函数的合成就是函数 $(f, g)\mapsto g\circ f$；而普通乘法、加法和减法分别是函数 $(x, y)\mapsto xy$，$(x, y)\mapsto x+y$，$(x, y)\mapsto x-y$. 由合成和减法的例子知我们为什么要选择有序对，这是因为 $x*y$ 和 $y*x$ 可能不相等. 像任何函数那样，运算也是单值的. 如果我们要明确说明这一点，我们通常称它为**替换律**：

$$\text{若 } x=x', y=y' \text{ 则 } x*y=x'*y'. \quad 125$$

→ **定义** *集合 G 带上运算 $*$ 和特殊元 $e\in G$(叫做* **单位元**) *称为* **群**，*如果*

(i) *结合律成立：对任意 $a, b, c\in G$ 有*

$$a*(b*c)=(a*b)*c;$$

(ii) *对所有 $a\in G$ 有 $e*a=a$；*

(iii) *对任意 $a\in G$，存在 $a'\in G$ 可使 $a'*a=e$.*

由命题 2.13 知，由集合 X 的所有置换构成的集合 S_X 带上合成运算和单位元(1)是一个群(称为 X 上的**对称群**).

我们现在处于代数成为抽象代数的转折点上. 与由 $X=\{1, 2, \cdots, n\}$ 的所有置换构成的具体群 S_n 相比，我们将证明群的一般结论而不详细说明它们的元素或运算. 因此，元素的积是否可计算也不是显然的，而是只服从某些法则. 我们将看到这个方法是十分有效的，这是因为许多定理适合于许多不同的群，证明这些定理不需要对每个群都证明一遍，所以证明的效率更高了. 例如，接下来的一个命题和三个引理给出了对每个群都成立的一些性质. 除了这个明显的节省之外，当我们处理特殊的具体群时，用“抽象”的观点会显得更简单. 例如，我们将看

到，在没有认出问题中的元素是置换时，S_n 的某些性质处理起来更简单(见例 2.52).

→ **定义** 群 G 称为**阿贝尔群**[⊖]，如果它满足**交换律**：对任意 x，$y\in G$ 有 $x*y=y*x$.

群 $S_n(n\geqslant 3)$不是阿贝尔群，因为 S_n 中元素$(1\ 2)$和$(1\ 3)$不能交换：$(1\ 2)(1\ 3)=(1\ 3\ 2)$而$(1\ 3)(1\ 2)=(1\ 2\ 3)$.

在给出群的例子之前，先来证明一些基本的事实.

我们怎样乘三个数？例如，给定表达式 $2\times3\times4$，我们可以先作 $2\times3=6$，然后 $6\times4=24$. 或者先作 $3\times4=12$，然后作 $2\times12=24$. 当然，两个结果相等，因为数的乘法满足结合律. 但是，并非所有运算都满足结合律. 例如，减法不满足结合律：若 $c\neq0$，则

$$a-(b-c)\neq(a-b)-c.$$

一般地，我们怎样乘三个元素 $a*b*c$？由于我们一次只可以乘两个元素，所以存在两种选择：
126 作乘法 $b*c$ 得到G 的一个新元素，然后用 a 乘这个新元素得到 $a*(b*c)$；或者，我们可以先作乘法 $a*b$，再用 c 乘这个新元素得到$(a*b)*c$. 结合律是说这两个结果相等，所以不用括号直接写 $a*b*c$ 不会产生歧义. 下面这个引理表明，一些结合律性质对含四个因子的积成立(定理 2.49 证明了，结合律允许我们对含 $n\geqslant3$ 个因子的积分配括号).

引理 2.43 若 $*$ 是集合 G 上满足结合律的运算，则对所有 a，b，c，$d\in G$ 有

$$(a*b)*(c*d)=[a*(b*c)]*d.$$

证明 若记 $g=a*b$，则$(a*b)*(c*d)=g*(c*d)=(g*c)*d=[(a*b)*c]*d=[a*(b*c)]*d$. ■

引理 2.44 若 G 是一个群，且 $a\in G$ 满足 $a*a=a$，则 $a=e$.

证明 存在 $a'\in G$ 满足 $a'*a=e$. 在 $a*a=a$ 的两边左乘 a'得 $a'*(a*a)=a'*a$. 右边是 e，左边是$a'*(a*a)=(a'*a)*a=e*a=a$，所以 $a=e$. ■

→ **命题 2.45** 设 G 是一个群，运算为 $*$，单位元为 e.

(i)对所有 $a\in G$，有 $a*a'=e$.

(ii)对所有 $a\in G$，有 $a*e=a$.

(iii)若 $e_0\in G$ 满足对所有 $a\in G$ 有 $e_0*a=a$，则 $e_0=e$.

(iv)设 $a\in G$. 若 $b\in G$ 满足 $b*a=e$，则 $b=a'$.

证明 (i)我们知道 $a'*a=e$，现在证明 $a*a'=e$. 由引理 2.43 知

$$\begin{aligned}(a*a')*(a*a')&=[a*(a'*a)]*a'\\&=(a*e)*a'\\&=a*(e*a')\\&=a*a'.\end{aligned}$$

由引理 2.44 知 $a*a'=e$.

(ii)利用(i)有

$$a*e=a*(a'*a)=(a*a')*a=e*a=a.$$

⊖ 这个术语是纪念阿贝尔的. 1827 年，他证明了若多项式根的伽罗瓦群是交换的则可以用公式求解根这一定理. 这个定理现在实际上被遗忘了，因为伽罗瓦在 1830 年的工作取代了它.

因此 $a*e=a$. 127

(iii)现在证明群有唯一的单位元，即群 G 中没有其他元素具有 e 在定义中的性质：对所有 $a\in G$ 有 $e*a=a$. 若对所有 $a\in G$ 有 $e_0*a=a$，则 $e_0*e_0=e_0$. 由引理 2.44 知 $e_0=e$.

(iv)在(i)中我们证明了若 $a'*a=e$ 则 $a*a'=e$. 于是

$$b=b*e=b*(a*a')=(b*a)*a'=e*a'=a'.$$ ■

由(iii)知对每个 $a\in G$，都有唯一的 $a'\in G$ 使 $a'*a=e$.

→ **定义** 设 G 是群，$a\in G$，则满足 $a'*a=e$ 的唯一元素 $a'\in G$ 称为 a 的**逆元**，记为 a^{-1}.

在所有群中还有下列三个性质.

→ **引理 2.46** 设 G 是一个群.

(i)**消去律**成立：设 a，b，$x\in G$，若 $x*a=x*b$ 或 $a*x=b*x$，则 $a=b$.

(ii)对所有 $a\in G$ 有 $(a^{-1})^{-1}=a$.

(iii)若 a，$b\in G$，则 $(a*b)^{-1}=b^{-1}*a^{-1}$.

证明 (i)$a=e*a=(x^{-1}*x)*a=x^{-1}*(x*a)=x^{-1}*(x*b)=(x^{-1}*x)*b=e*b=b$. 当 x 在右边时，可以类似地证明结论.

(ii)由命题 2.45(i)知 $a*a^{-1}=e$. 又由命题 2.45(iv)中逆元的唯一性知 $(a^{-1})^{-1}$ 是满足 $x*a^{-1}=e$ 的唯一元素 $x\in G$. 因此 $(a^{-1})^{-1}=a$.

(iii)由引理 2.43 知

$$(a*b)*(b^{-1}*a^{-1})=[a*(b*b^{-1})]*a^{-1}=(a*e)*a^{-1}=a*a^{-1}=e.$$

由命题 2.45(iv)知 $(a*b)^{-1}=b^{-1}*a^{-1}$. ■

在上面给出的证明中，我们很小心地证明了每一步并展示了所有的括号，因为我们还只是刚开始学习群论的思想. 但是，当我们开始熟练时，写出所有这样的细节就没有必要了. 这不是说我们可以变得粗心了，只是说我们正在变得成熟. 当然，当你的证明受到挑战时，你必须 128 做好准备给出省略的细节.

从现在开始，我们通常用 ab 记群中的乘积 $a*b$(在对称群中，我们总是把 $\alpha\circ\beta$ 缩写为 $\alpha\beta$)，并且不用 e 而用 1 记单位元. 但是，当一个群是阿贝尔群时，我们经常使用**加法记号**. 以下是用加法记号写出的群的定义.

一个**加法群**是指一个集合 G 带上一个运算＋和一个单位元 $0\in G$ 满足

(i)对所有 a，b，$c\in G$ 有 $a+(b+c)=(a+b)+c$；

(ii)对所有 $a\in G$ 有 $0+a=a$；

(iii)对每个 $a\in G$，存在 $-a\in G$，满足 $(-a)+a=0$.

注意，在加法记号中，a 的逆元不记为 a^{-1}，而记为 $-a$.

下面给出了群的许多例子(还有更多!). 浏览一下，选出感兴趣的一两个认真看看.

→ **例 2.47** (i)我们提醒读者，集合 X 的所有置换构成的集合 S_X 在合成运算下是一个群. 特别地，$X=\{1, 2, \cdots, n\}$的所有置换构成的集合 S_n 是一个群.

(ii)整数集$\mathbb{Z}$ 是一个加法阿贝尔群，其中 $a*b=a+b$，单位元 $e=0$，整数 n 的逆元为 $-n$. 类似地，我们可以看出$\mathbb{Q}$，$\mathbb{R}$ 和$\mathbb{C}$ 都是加法阿贝尔群.

(iii)所有非零有理数构成的集合$\mathbb{Q}^{\times}$是一个阿贝尔群，其中 $*$ 是普通乘法，数 1 是单位元，$r\in\mathbb{Q}^{\times}$的逆元是 $1/r$. 类似地，$\mathbb{R}^{\times}$和$\mathbb{C}^{\times}$都是乘法阿贝尔群.

注意，$\mathbb{Z}^{\times}$不是群，因为它的任何元素(除了±1)在$\mathbb{Z}^{\times}$中没有乘法逆元.

(iv)中心为原点半径为 1 的圆 S^1 可以看成一个乘法阿贝尔群，若我们把它的点看作是模为 1 的复数. **圆群**定义为

$$S^1=\{z\in\mathbb{C}:|z|=1\},$$

其中运算是复数的乘法，这是 S^1 上的一个运算，来自推论 1.23. 当然，复数的乘法是满足结合律的，单位元是 1(其模为 1)，且任何模为 1 的复数的逆元是它的复共轭，其模也为 1. 因此，S^1

129 是一个群. 即使 S^1 是一个阿贝尔群，我们仍然用乘法来写它，因为用加法写会产生麻烦.

(v)对任意正整数 n，设

$$\Gamma_n=\{\zeta^k:0\leqslant k<n\}$$

是所有 n 次单位根构成的集合，其中

$$\zeta=e^{2\pi i/n}=\cos(2\pi/n)+i\sin(2\pi/n).$$

读者可以利用棣莫弗定理看出 Γ_n 带上复数乘法是一个阿贝尔群. 而且，任何单位根的逆元都是它的复共轭.

(vi)平面$\mathbb{R}\times\mathbb{R}$带上向量加法是一个加法阿贝尔群，即若$\boldsymbol{v}=(x,y)$，$\boldsymbol{v}'=(x',y')$，则$\boldsymbol{v}+\boldsymbol{v}'=(x+x',y+y')$. 单位元是原点 $O=(0,0)$，$\boldsymbol{v}=(x,y)$的逆元是$-\boldsymbol{v}=(-x,-y)$.

(vii)**奇偶群**$\mathcal{P}$有两个元素“偶”和“奇”，其运算是

$$偶+偶=偶=奇+奇$$

和

$$偶+奇=奇=奇+偶.$$

读者可以证明$\mathcal{P}$是一个阿贝尔群.

(viii)设 X 是一个集合. 回忆一下，若 A 和 B 是 X 的子集，则它们的对称差是 $A+B=(A-B)\cup(B-A)$(对称差在图 2-6 中有描述). **布尔群**$B(X)$[以逻辑学家布尔(G. Boole, 1815—1864)的名字命名]是指 X 的所有子集构成的族带上对称差运算.

显然，$A+B=B+A$，所以对称差是交换的. 单位元是空集$\varnothing$，A 的逆元是 A 本身，因为$A+A=\varnothing$(见习题 2.4). 因此，$B(X)$是一个阿贝尔群. ◀

→ **例 2.48** (i)一个(2×2 实)**矩阵**[⊖] A 是$\begin{bmatrix}a & c\\ b & d\end{bmatrix}$，其中 $a,b,c,d\in\mathbb{R}$. 若 $B=\begin{bmatrix}w & y\\ x & z\end{bmatrix}$，则积 AB 定义为

130
$$AB=\begin{bmatrix}a & c\\ b & d\end{bmatrix}\begin{bmatrix}w & y\\ x & z\end{bmatrix}=\begin{bmatrix}aw+cx & ay+cz\\ bw+dx & by+dz\end{bmatrix}.$$

元素 a,b,c,d 称为 A 的元素. 称(a,c)为 A 的第一行，称(b,d)为第二行；称(a,b)为 A

⊖ “矩阵(matrix)”(由意思为“母亲”的单词导出的)在拉丁文中的意思是“子宫”. 一般地，它是指包含事物本质的东西. 它的数学用法是由一个 2×2 矩阵产生的，2×2 矩阵就是四个数构成的一个阵列，该阵列完全描述了一类称为线性变换的函数$\mathbb{R}^2\to\mathbb{R}^2$(一般地，更大的矩阵包含高维空间之间的线性变换的本质).

的第一列，(c, d)为第二列. 因此，积 AB 的每个元素是 A 的一行和 B 的一列的点积. A 的**行列式**，记为 $\det(A)$，是数 $ad-bc$. 矩阵 A 称为**非奇异的**，若 $\det(A)\neq 0$. 读者可以计算得

$$\det(AB) = \det(A)\det(B),$$

由此得非奇异矩阵的积是非奇异的. 所有非奇异矩阵构成的集合 $GL(2, \mathbb{R})$带上矩阵乘法是一个(非阿贝尔)群，称为 2×2 **实一般线性群**：单位元是单位矩阵

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

非奇异矩阵 A 的逆元是

$$A^{-1} = \begin{bmatrix} d/\Delta & -c/\Delta \\ -b/\Delta & a/\Delta \end{bmatrix},$$

其中 $\Delta = ad-bc = \det(A)$. (结合律的证明尽管很麻烦，但却是常规的. 一旦我们知道了矩阵和线性变换之间的关系[见推论 4.72]就可以给出结合律的一个"简洁"证明).

(ii)前面这个例子可以从两个方面修改. 首先，我们可以允许元素属于$\mathbb{Q}$或$\mathbb{C}$，这就给出了群 $GL(2, \mathbb{Q})$或 $GL(2, \mathbb{C})$. 我们甚至可以允许元素属于$\mathbb{Z}$，此时定义 $GL(2, \mathbb{Z})$为所有行列式为± 1 的矩阵构成的集合(我们想要 A^{-1}的所有元素都在$\mathbb{Z}$ 中). 读者应当十分熟悉线性代数，所有非奇异 $n\times n$ 矩阵带上矩阵乘法构成群 $GL(n, \mathbb{R})$.

(iii)所有**特殊**[⊖]**正交**矩阵，即所有形如

$$A = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

的矩阵构成一个群，记为 $SO(2, \mathbb{R})$，并称为 2×2 **特殊正交群**. 让我们证明矩阵乘法是 $SO(2, \mathbb{R})$上的一个运算. 积

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

是

$$\begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -[\cos\alpha\sin\beta + \sin\alpha\cos\beta] \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{bmatrix}.$$ 131

正弦和余弦的加法定理表明这个积还是一个特殊正交矩阵，因为它等于

$$\begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}.$$

实际上，这个计算表明 $SO(2, \mathbb{R})$是阿贝尔群. 显然，单位矩阵是特殊正交的，我们让读者检验一个特殊正交矩阵的逆元(因为特殊正交矩阵的行列式为 1，所以逆元存在)也是特殊正交的.

在习题 2.77 中，我们看到 $SO(2, \mathbb{R})$是与圆群 S^1 同构的群，且这个群由平面绕原点的所有旋转构成.

(iv)**仿射**[⊜]**群** $\mathrm{Aff}(1, \mathbb{R})$是由所有形如

⊖ 形容词"特殊的"修饰矩阵，通常是指矩阵的行列式为 1.

⊜ 射影几何通过添加"无穷远点"扩充平面(和高维空间). 被扩充的平面称为射影平面，原来的平面称为仿射(或有限)平面. 仿射函数是仿射平面之间的特殊函数.

$$f_{a,b}(x) = ax + b$$

的函数 $f: \mathbb{R} \to \mathbb{R}$（称为仿射映射）构成的，其中 a 和 b 是固定的实数，且 $a \neq 0$. 让我们检验 Aff(1, $\mathbb{R}$)带上合成运算作成一个群. 若 $f_{c,d}(x) = cx + d$，则

$$\begin{aligned} f_{a,b}f_{c,d}(x) &= f_{a,b}(cx + d) \\ &= a(cx + d) + b \\ &= acx + (ad + b) \\ &= f_{ac,ad+b}(x). \end{aligned}$$

由于 $ac \neq 0$，所以合成是一个仿射映射. 恒等函数 $1_{\mathbb{R}}: \mathbb{R} \to \mathbb{R}$ 是仿射映射($1_{\mathbb{R}} = f_{1,0}$)，容易看出 $f_{a,b}$的逆元是 $f_{a^{-1},-a^{-1}b}$. 读者应当注意到这个合成是矩阵乘法：

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ac & ad + b \\ 0 & 1 \end{bmatrix}.$$

类似地，用$\mathbb{Q}$替换$\mathbb{R}$得到 Aff(1, $\mathbb{Q}$)，用$\mathbb{C}$替换$\mathbb{R}$得到 Aff(1, $\mathbb{C}$). ◀

下面的讨论是技巧性的，若读者知道了定理 2.49，则可以跳过这一部分. 非正式地讲，
132 这个定理是说，若一个运算满足结合律，则在含有 $n \geqslant 3$ 个因子的积中不需要用括号.

设 G 是一个集合，带一个二元运算. n-元组$(a_1, a_2, \cdots, a_n) \in G \times \cdots \times G$ 称为 **n 元表达式**(含有 n 个因子)，它通过下述方法产生 G 的许多元素. 选取两个相邻的因子相乘，得到一个$(n-1)$元表达式：刚得到的新积和原来的 $n-2$ 个因子. 在这个更短的新表达式中，选取两个相邻因子(或是原来的两个因子或是原来的一个因子与第一步中得到的新积)相乘. 重复这一过程直到得到一个 2 元表达式(W, X)，它们相乘得到 G 的一个元素 WX. 称 WX 为由原始表达式导出的**最终积**. 例如，考虑 4 元表达式(a, b, c, d). 我们可以先作乘法 ab，得到 3 元表达式(ab, c, d). 现在选取一对 ab，c 或 c，d. 不管那种选法，让它们相乘得到 2 元表达式$((ab)c, d)$或(ab, cd). 这两个表达式中的两个因子可以乘起来得到最终积$[(ab)c]d$ 或$(ab)(cd)$. 由(a, b, c, d)导出的其他最终积可通过第一步作乘法 bc 或 cd 产生. 一个运算满足结合律，是说由 3 元表达式产生的两个最终积相等. 即使一个运算满足结合律，从一个较长表达式导出的所有最终积是否相等，也不是很明显.

定义 一个 n 元表达式$(a_1, a_2, \cdots, a_n)$**不需要用括号**，若它导出的所有最终积都相等，即不管怎样选取相邻因子相乘，得到的所有积在 G 中都是相等的.

定理 2.49(广义结合律) 若 $n \geqslant 3$，则群 G 中每个 n 元表达式$(a_1, a_2, \cdots, a_n)$不需要用括号.

注 注意，证明中将不会用到单位元和逆元. 因此，定理的前提条件可以减弱为假设 G 只是一个半群，即 G 是一个非空集合，带着一个满足结合律的二元运算.

证明 用(第二)归纳法证明. 基础步骤 $n=3$ 由结合律得到. 对于归纳步骤，考虑 G 的通过两种一系列的选取从 n 元表达式$(a_1, a_2, \cdots, a_n)$中得到的 2 元表达式：

$$(W, X) = (a_1 \cdots a_i, a_{i+1} \cdots a_n) \quad 和 \quad (Y, Z) = (a_1 \cdots a_j, a_{j+1} \cdots a_n).$$

我们必须证明，$WX = YZ$ 在 G 中成立. 由归纳法，$W = a_1 \cdots a_i$，$X = a_{i+1} \cdots a_n$，$Y = a_1 \cdots a_j$，$Z = a_{j+1} \cdots a_n$，都是从 $m(m<n)$元表达式中得到的最终积(有且仅有一个). 为不失一般性，我
133 们可以假设 $i \leqslant j$. 若 $i = j$，则由归纳假设知 $W = Y$ 和 $X = Z$ 在 G 中成立，所以 $WX = YZ$.

我们现在可以假设 $i<j$. 设 A 是 i 元表达式$(a_1, \cdots, a_i)$的一个最终积，设 B 是从表达式$(a_{i+1}, \cdots, a_j)$中得到的最终积，设 C 是从表达式 $a_{j+1}, \cdots, a_n$ 中得到的最终积. 群元素 A、B 和 C 是被明确定义了的，因为归纳假设是说每个较短表达式只产生一个最终积. 现在 $W=A$，因为两个都是从 i 元表达式$(a_1, \cdots, a_i)$中产生的最终积，$Z=C$[两个都是从$(n-j)$元表达式$(a_{j+1}, \cdots, a_n)$中产生的最终积]，$X=BC$[两个都是从$(n-i)$元表达式$(a_{i+1}, \cdots, a_n)$中产生的最终积]，$Y=AB$[两个都是从 j 元表达式$(a_1, \cdots, a_j)$中产生的最终积]. 我们得到 $WX=A(BC)$，$YZ=(AB)C$，所以结合律和基础步骤 $n=3$ 给出 $WX=YZ$，证毕. ■

→ **定义** 若 G 是一个群，$a\in G$，则对 $n\geqslant 1$ 归纳地定义幂[⊖] a^n：

$$a^1=a \quad 和 \quad a^{n+1}=aa^n.$$

定义 $a^0=1$，若 n 是一个正整数，则定义

$$a^{-n}=(a^{-1})^n.$$

我们让读者证明$(a^{-1})^n=(a^n)^{-1}$，这是引理 2.46(iii)中等式的一个特殊情形.

这里隐藏着一个问题. 一次和二次幂很好：$a^1=a$，$a^2=aa$. 三次幂有两种可能：我们已经定义了 $a^3=aa^2=a(aa)$，但是存在另一种合理的备选者：$(aa)a=a^2a$. 若我们假设结合律成立，则它们相等：

$$a^3=aa^2=a(aa)=(aa)a=a^2a.$$

广义结合律表明一个元素的所有次幂是被明确定义的.

推论 2.50 若 G 是一个群，$a\in G$，m，$n\geqslant 1$，则

$$a^{m+n}=a^ma^n \quad 和 \quad (a^m)^n=a^{mn}.$$

证明 a^{m+n}和 a^ma^n 都是从含 $m+n$ 个等于 a 的因子的表达式中产生的；在第二个等式中，$(a^m)^n$ 和 a^{mn}都是从含 mn 个等于 a 的因子的表达式中产生的. ■ 134

于是，在群中元素 a 的任何两个幂是交换的：

$$a^ma^n=a^{m+n}=a^{n+m}=a^na^m.$$

下面这个命题有各种各样的证法，尽管都很直接明白，但是过程很长.

→ **命题 2.51(指数律)** 设 G 是一个群，a，$b\in G$，m 和 n 都是整数(不一定是正的).

(i)若 a 和 b 交换，则$(ab)^n=a^nb^n$.

(ii)$(a^n)^m=a^{mn}$.

(iii)$a^ma^n=a^{m+n}$.

证明 留给读者作练习. ■

记号 a^n 自然是表示 $a*a*\cdots*a$，其中 a 出现 n 次. 但是，若运算是+，则用 na 记 $a+a+\cdots+a$更自然些. 设 G 是用加法写的群，若 a，$b\in G$，且 m 和 n 都是整数(不一定是正的)，则命题 2.51 通常写为：

⊖ 术语“x 平方(x square)”和“x 立方(x cube)”起源于几何学. 在这个背景下，术语“幂(power)”的使用要追溯到欧几里得，他写道：“直线的幂是这条直线的平方”(来自 1570 年比林斯利(H. Billingsley)翻译的第一个欧几里得英文译本). “幂”是希腊词“dunamis”在欧洲语中的标准解释. 但是，与欧几里得同时代人，例如亚里士多德和柏拉图，经常用“dunamis”表示“扩大”的含义，这看起来是一个更合适的变换，因为欧几里得可能正在思考一条掠过 2-维正方形的 1-维直线.(我感谢唐娜·夏乐韦(Donna Shalev)告诉了我 dunamis 的经典用法.)

(i) $n(a+b)=na+nb$.

(ii) $m(na)=(mn)a$.

(iii) $ma+na=(m+n)a$.

例 2.52 假设洗一副纸牌，使得纸牌的顺序由 1，2，3，4，…，52 变为 2，1，4，3，…，52，51. 若按同样的方法再洗一遍，则纸牌回到原来的顺序. 对 52 张牌的任意置换 α，类似的事情都会发生：若我们将 α 重复足够多的次数，则纸牌最终会恢复为原来的顺序. 为了弄明白这一点，要用到置换的知识. 把 α 写成一些不相交循环置换的积，不妨设 $\alpha=\beta_1\beta_2\cdots\beta_t$，其中 β_i 是一个 r_i-循环置换. 根据习题 2.25，对每个 i 有 $\beta_i^{r_i}=(1)$，所以 $\beta_i^k=(1)$，其中 $k=r_1\cdots r_t$. 因为不相交循环置换交换，所以由习题 2.30 知

$$\alpha^k=(\beta_1\cdots\beta_t)^k=\beta_1^k\cdots\beta_t^k=(1).$$

以下是更一般的结果，其证明更简单(抽象代数可能比代数更容易些)：若 G 是一个有限群且 $a\in G$，则对某个 $k\geqslant 1$ 有 $a^k=1$. 我们利用引理 2.23(i)中的讨论. 考虑子集

135 $$1,a,a^2,\cdots,a^n,\cdots.$$

由于 G 是有限的，在这个无限序列中一定有某个重复会发生：存在整数 $m>n$ 满足 $a^m=a^n$，因而 $1=a^ma^{-n}=a^{m-n}$. 我们已经证明了存在 a 的某个正次幂等于 1. 我们最初对 52 张牌的置换 α 有 $\alpha^k=(1)$ 的讨论不是没有用的，因为命题 2.55 将表明，我们可以选择 $k=\operatorname{lcm}(r_1,\cdots,r_t)$. ◀

定义 设 G 是一个群，$a\in G$. 若对某个 $k\geqslant 1$ 有 $a^k=1$，则这样的最小指数 $k\geqslant 1$ 称为 a 的**阶**；若这样的幂不存在，则我们称 a 有**无限阶**.

例 2.52 中的讨论表明，在有限群中每个元素都有有限阶. 在任意群 G 中，单位元的阶为 1，且是群 G 中阶为 1 的唯一元素. 一个元素阶为 2 当且仅当它等于它的逆元. 矩阵 $A=\begin{bmatrix}1&1\\0&1\end{bmatrix}$在群 $GL(2,\mathbb{R})$中有无限阶，因为对所有 $k\geqslant 1$ 有 $A^k=\begin{bmatrix}1&k\\0&1\end{bmatrix}\neq\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

引理 2.53 设 G 是一个群，$x\in G$ 有有限阶 k. 若 $x^n=1$，则 $k\mid n$.

证明 根据除法算式，$n=qk+r$，其中 $0\leqslant r<k$. 因而

$$1=x^n=x^{qk+r}=(x^k)^qx^r=x^r.$$

由于 $x^r=1$ 和 $r<k$，我们一定有 $r=0$，即 $k\mid n$. ■

引理 2.53 有另一种证明，它表明群元素的阶和理想之间存在联系. 理想是$\mathbb{Z}$ 的子集，是在证明最大公因数是线性组合时产生的.

命题 2.54 设 G 是一个群，并假设 $x\in G$ 有有限阶 k.

(i) $I=\{n\in\mathbb{Z}: x^n=1\}$是 k 的所有倍数构成的集合.

(ii) 若 $x^n=1$，则 $k\mid n$.

证明 (i)我们证明 I 满足推论 1.37 的假设：

(a)：$0\in I$，因为 $x^0=1$.

(b)：若 n，$m\in I$，则 $x^n=1$，$x^m=1$，所以 $x^{n-m}=x^nx^{-m}=1$，因而 $n-m\in I$.

(c)：若 $n\in I$，$q\in\mathbb{Z}$，则 $x^n=1$，$x^{qn}=(x^n)^q=1$，因而 $qn\in I$.

因此，I 由 d 的所有倍数构成，其中 d 是 I 中的最小正整数. 但是，根据定义，x 的阶 k 是这样的最小正整数，所以 $d=k$.

(ii)若 $x^n=1$，则 $n\in I=(k)$，所以 $k\mid n$. ■ 136

S_n 中置换的阶是多少?

→ **命题 2.55** 设 $\alpha\in S_n$.

(i)若 α 是一个 r-循环置换，则 α 的阶为 r.

(ii)若 $\alpha=\beta_1\cdots\beta_t$ 是不相交的 r_i-循环置换 β_i 的积，则 α 的阶 $m=\operatorname{lcm}\{r_1, \cdots, r_t\}$.

(iii)若 p 是素数，则 α 的阶为 p 当且仅当它是一个 p-循环置换或是不相交的 p-循环置换的积.

证明 (i)这是习题 2.25(i).

(ii)根据(i)，每个 β_i 有阶 r_i. 假设 $\alpha^M=(1)$. 由于 β_i 交换，所以 $(1)=\alpha^M=(\beta_1\cdots\beta_t)^M=\beta_1^M\cdots\beta_t^M$. 根据习题 2.31(ii)，这些 β_i 的不相交性表明对每个 i 有 $\beta_i^M=(1)$，所以由引理 2.53 知对所有 i 有 $r_i\mid M$，即 M 是 $r_1, \cdots, r_t$ 的一个公倍数. 但是，若 $m=\operatorname{lcm}\{r_1, \cdots, r_t\}$，则容易看出 $\alpha^m=(1)$. 因此，α 的阶为 m.

(iii)把 α 写成不相交循环置换的积并利用(ii)可得. ■

例如，S_n 中置换的阶为 2 当且仅当它是一个对换或是不相交对换的积.

我们现在可以讨论例 2.30 中的表 2-2.

表 2-3 S_5 中的置换

循环结构	个数	阶	奇偶性
(1)	1	1	偶
(1 2)	10	2	奇
(1 2 3)	20	3	偶
(1 2 3 4)	30	4	奇
(1 2 3 4 5)	24	5	偶
(1 2)(3 4 5)	20	6	奇
(1 2)(3 4)	15	2	偶
	120		

对称

我们现在给出群和对称之间的联系(我们将利用ℝ上的一些线性代数). 当我们说一个等腰三角形△是对称的，其含义是什么呢? 图 2-10 表明，△=△ABC，其底边 AB 在 x 轴上，y 轴是 AB 的垂直平分线. 137 闭上眼睛，让△在 y 轴上被反射(使得顶点 A 和 B 互换). 睁开眼睛，你不能说出△已经被反射了，因此△关于 y 轴对称. 另一方面，若△在 x 轴上被反射，则睁开眼睛时，很明显地发现一个反射已经发生，因此△关于 x 轴不对称. 反射是一种特殊的等距同构.

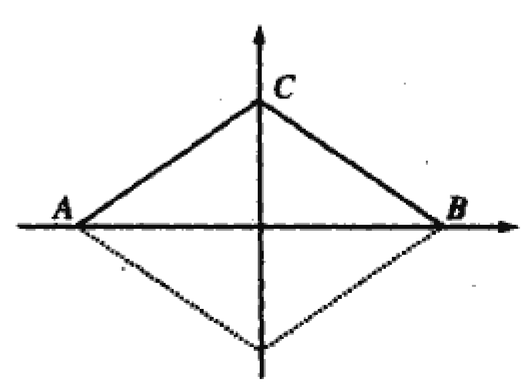


图 2-10 等腰三角形

→ **定义** 平面的一个**等距同构**是指保持距离的函数 $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$：对 $\mathbb{R}^2$ 中的所有点 $P=(a, b)$ 和 $Q=(c, d)$，有

$$\|\varphi(P)-\varphi(Q)\| = \|P-Q\|,$$

其中 $\|P-Q\|=\sqrt{(a-c)^2+(b-d)^2}$ 是 P 到 Q 的距离.

用 $P\cdot Q$ 表示点积：

$$P\cdot Q=(a,b)\cdot(c,d)=ac+bd.$$

现在

$$\begin{aligned}(P-Q)\cdot(P-Q) &= P\cdot P-2(P\cdot Q)+Q\cdot Q\\ &= (a^2+b^2)-2(ac+bd)+(c^2+d^2)\\ &= (a^2-2ac+c^2)+(b^2-2bd+d^2)\\ &= (a-c)^2+(b-d)^2\\ &= \|P-Q\|^2.\end{aligned}$$

138

引理 2.56 设 φ 是平面的一个等距同构. 则 φ 保持点积不变[即，对所有点 P 和 Q 有 $\varphi(P)\cdot\varphi(Q)=P\cdot Q$]当且仅当 $\varphi(O)=O$.

证明 若 $\varphi(P)\cdot\varphi(Q)=P\cdot Q$ 对所有点 P 和 Q 成立，则 $\varphi(O)\cdot\varphi(O)=O\cdot O=0$. 于是 φ 固定原点，这是因为若 $\varphi(O)\neq O$，则 $\varphi(O)\cdot\varphi(O)=\|\varphi(O)\|^2\neq 0$.

反之，若 $\varphi(O)=O$，则对所有 P 有

$$\|P\| = \|P-O\| = \|\varphi(P)-\varphi(O)\| = \|\varphi(P)\|,$$

因为 φ 是一个等距同构. 因而，对所有点 P 和 Q 有

$$\begin{aligned}\|\varphi(P)\|^2+\|\varphi(Q)\|^2-2\varphi(P)\varphi(Q) &= [\varphi(P)-\varphi(Q)]\cdot[\varphi(P)-\varphi(Q)]\\ &= \|\varphi(P)-\varphi(Q)\|^2\\ &= \|P-Q\|^2\\ &= (P-Q)\cdot(P-Q)\\ &= \|P\|^2+\|Q\|^2-2P\cdot Q.\end{aligned}$$

因此 $\varphi(P)\cdot\varphi(Q)=P\cdot Q$ ■

回忆一个公式，它给出了点积的几何解释：

$$P\cdot Q=\|P\|\,\|Q\|\cos\theta,$$

其中 θ 是 P 和 Q 之间的夹角. 于是每个等距同构是保角的. 特别地，P 和 Q 是正交的当且仅当 $P\cdot Q=0$，所以等距同构保正交性. 反之，若 $\varphi(P)\cdot\varphi(Q)=P\cdot Q$，即 φ 保持点积不变，则公式 $(P-Q)\cdot(P-Q)=\|P-Q\|^2$ 表明 φ 是一个等距.

我们记平面的所有等距同构构成的集合为 $\mathbf{Isom}(\mathbb{R}^2)$；由所有满足 $\varphi(O)=O$ 的等距同构 φ 构成的子集，称为平面的**正交群**，记为 $O(2, \mathbb{R})$. 我们将在命题 2.61 中看到，$\mathbf{Isom}(\mathbb{R}^2)$ 和 $O(2, \mathbb{R})$ 对合成运算构成群.

我们介绍一些记号以帮助我们分析等距同构.

记号 设 P 和 Q 是平面上不同的两点，用 $L[P, Q]$ 表示它们确定的直线，用 PQ 表示端点为 P 和 Q 的直线段.

以下是等距同构的一些例子.

例 2.57 (i)给定角 θ，绕原点 O 的**旋转** R_θ 定义如下：$R_\theta(O)=O$；若 $P\neq O$，则在图 2-11 中画直线段 PO，将它旋转 θ 到 OP'(若 θ 是正数则逆时针旋转，若 θ 是负数则顺时针旋转)，定义 $R_\theta(P)=P'$. 当然，我们可以绕平面中的任何一点旋转. 139

(ii)定义直线 L 的**反射** ρ_L(L 称为它的轴)为：它固定 L 中的每一点；若 $P\notin L$，则 $\rho_L(P)=P'$，如图 2-12 所示(L 是 PP' 的中垂线). 若我们假设 L 是一面镜子，则 P' 是 P 的镜像. 现在 $\rho_L\in \mathbf{Isom}(\mathbb{R}^2)$. 若 L 过原点，则 $\rho_L\in O(2, \mathbb{R})$.

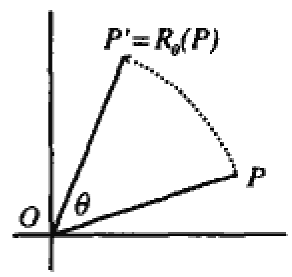


图 2-11 旋转

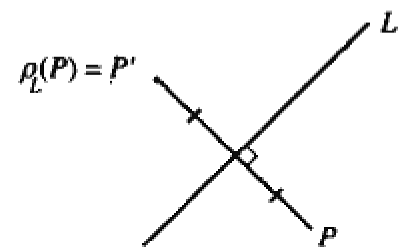


图 2-12 反射

(iii)给定一点 V，**沿 V 的平移**[⊖]是指函数 $\tau_V: \mathbb{R}^2\to\mathbb{R}^2$，$\tau_V(U)=U+V$. 平移属于 $\mathbf{Isom}(\mathbb{R}^2)$. 平移 τ_V 固定原点当且仅当 $V=O$，所以恒等函数既是旋转又是平移. ◀

命题 2.58 *若 φ 是平面的一个等距同构，则 $\mathbb{R}^2$ 中的不同点 P，Q，R 共线当且仅当 $\varphi(P)$，$\varphi(Q)$，$\varphi(R)$ 共线. 因而，若 L 是一条直线，则 $\varphi(L)$ 也是一条直线.*

证明 设 P，Q，R 共线. 选取记号使得 R 在 P 和 Q 之间. 因而 $\|P-Q\|=\|P-R\|+\|R-Q\|$. 假设 $\varphi(P)$，$\varphi(Q)$，$\varphi(R)$ 不共线，则它们是一个三角形的顶点. 由三角不等式得

$$\|\varphi(P)-\varphi(Q)\| < \|\varphi(P)-\varphi(R)\| + \|\varphi(R)-\varphi(Q)\|,$$

与 φ 保距矛盾. 类似的讨论可证明反过来也成立. 假设 P，Q，R 不共线，则它们是一个三角形的顶点. 若 $\varphi(P)$，$\varphi(Q)$，$\varphi(R)$ 共线，则上述严格不等式变成了等式，与 φ 保距矛盾.

若 $\varphi(L)$ 不是直线，则它含有 3 个不共线的点 $\varphi(P)$，$\varphi(Q)$，$\varphi(R)$，其中 P，Q，R 位于 L 上，矛盾. ■

每个等距同构 φ 是一个单射. 若 $P\neq Q$，则 $\|P-Q\|\neq 0$，所以 $\|\varphi(P)-\varphi(Q)\|=\|P-Q\|\neq 0$，因而 $\varphi(P)\neq\varphi(Q)$. 虽然等距同构是满射不那么明显，但我们很快就会知道这一点. 140

命题 2.59 *$\mathbb{R}^2$ 的每个固定原点的等距同构 φ 是一个线性变换.*

证明 设 $C_d=\{Q\in\mathbb{R}^2: \|Q-O\|=d\}$ 是中心为 O 半径为 $d>0$ 的圆. 我们断言 $\varphi(C_d)\subseteq C_d$. 若 $P\in C_d$，则 $\|P-O\|=d$. 由于 φ 保距，所以 $d=\|\varphi(P)-\varphi(O)\|=\|\varphi(P)-O\|$；因此 $\varphi(P)\in C_d$.

设 $P\neq O$ 是 $\mathbb{R}^2$ 中的一点，并设 $r\in\mathbb{R}$. 若 $\|P-O\|=p$，则 $\|rP-O\|=|r|p$. 因而 $rP\in L[O, P]\cap C_{|r|p}$，其中 $C_{|r|p}$ 是中心为 O 半径为 $|r|p$ 的圆. 由引理 2.58 知，φ 保共

⊖ “平移(translation)”来自意思是“移动”的拉丁词. 它通常是指由一种语言变到另一种语言，但是这里它是指将一个点移动到另一个点上.

线，所以 $\varphi(L[O,P]\cap C_{|r|p})\subseteq L[O,\varphi(P)]\cap C_{|r|p}$，即 $\varphi(rP)=\pm r\varphi(P)$(因为一条直线与一个圆最多相交两点).

若我们排除 $\varphi(rP)=-r\varphi(P)$的可能性，则可以得到 $\varphi(rP)=r\varphi(P)$. 在 $r>0$ 的情形中，原点 O 位于 $-rP$ 和 P 之间，所以 $-rP$ 到 P 的距离是 $rp+p$. 另一方面，rP 到 P 的距离是 $|rp-p|$(若 $r>1$，则距离是 $rp-p$；若 $0<r<1$，则距离是 $p-pr$). 但是 $r+rp\neq|rp-p|$，所以 $\varphi(rP)\neq-r\varphi(P)$(因为 φ 保距). $r<0$ 的情形可作类似讨论.

最后只要证明 $\varphi(P+Q)=\varphi(P)+\varphi(Q)$. 若 O，P，Q 共线，则在直线 $L[O,P]$上选取一点 U 使它到原点的距离为 1. 因此，$P=pU$，$Q=qU$，$P+Q=(p+q)U$. 点 $O=\varphi(O)$，$\varphi(U)$，$\varphi(P)$，$\varphi(Q)$共线. 由于 φ 保持标量乘法，所以有

$$\begin{aligned}\varphi(P)+\varphi(Q)&=\varphi(pU)+\varphi(qU)\\&=p\varphi(U)+q\varphi(U)\\&=(p+q)\varphi(U)\\&=\varphi((p+q)U)\\&=\varphi(P+Q).\end{aligned}$$

若 O，P，Q 不共线，则由平行四边形法则得 $P+Q$：$P+Q$ 是点 S，使得 O，P，Q，S 是一个平行四边形的顶点. 由于 φ 保距，所以点 $O=\varphi(U)$，$\varphi(P)$，$\varphi(Q)$，$\varphi(S)$是一个平行四边形的顶点，所以 $\varphi(S)=\varphi(P)+\varphi(Q)$. 但是 $S=P+Q$，所以 $\varphi(P+Q)=\varphi(P)+\varphi(Q)$，证毕. ■

推论 2.60 每个等距同构 $\varphi:\mathbb{R}^2\to\mathbb{R}^2$ 都是一个双射，且每个固定 0 的等距同构是一个非奇异的线性变换.

证明 我们先假设 φ 固定原点：$\varphi(0)=0$. 由命题 2.59 知，φ 是一个线性变换. 因为 φ 是单射，所以 $P=\varphi(e_1)$，$Q=\varphi(e_2)$是$\mathbb{R}^2$ 的一个基，其中 $e_1=(1,0)$，$e_2=(0,1)$是$\mathbb{R}^2$ 的标准基. 于是函数 $\psi:\mathbb{R}^2\to\mathbb{R}^2$，$\varphi:aP+bQ\mapsto ae_1+be_2$，是单值的，且 ψ 和 φ 互为反函数. 因此，
141 φ 是一个双射，因而它是非奇异的.

假设 φ 是任一等距同构，使得 $\varphi(0)=U$. 因为 $\tau_{-U}\circ\varphi:0\mapsto U\mapsto 0$，所以 $\tau_{-U}\circ\varphi=\theta$，其中 θ 是一个非奇异线性变换. 因此 $\varphi=\tau_U\circ\theta$ 是一个双射，因为它是两个双射的合成. ■

我们将在第六章更仔细地研究 $\mathbf{Isom}(\mathbb{R}^2)$. 特别地，我们将看到，所有等距同构或是旋转、或是反射、或是平移、或是第四类、或滑动反射.

→ **定义** 正交群 $O(2,\mathbb{R})$是指由平面的固定原点的所有等距同构构成的集合.

命题 2.61 $\mathbf{Isom}(\mathbb{R}^2)$和 $O(2,\mathbb{R})$都在合成运算下构成群.

证明 我们证明 $\mathbf{Isom}(\mathbb{R}^2)$是一个群. 显然，$1_{\mathbb{R}^2}$ 是一个等距同构，因此 $1_{\mathbb{R}^2}\in\mathbf{Isom}(\mathbb{R}^2)$. 设 φ'和 φ 都是等距同构. 对所有点 P 和 Q，我们有

$$\begin{aligned}\|(\varphi'\varphi)(P))-(\varphi'\varphi)(Q))\|&=\|\varphi'(\varphi(P))-\varphi'(\varphi(Q))\|\\&=\|\varphi(P)-\varphi(Q)\|=\|P-Q\|,\end{aligned}$$

所以 $\varphi'\varphi$ 也是一个等距同构，即合成是 $\mathbf{Isom}(\mathbb{R}^2)$上的一个运算. 若 $\varphi\in\mathbf{Isom}(\mathbb{R}^2)$，则由推论 2.60 知，$\varphi$ 是一个双射，所以它有反函数 φ^{-1}. 现在 φ^{-1}也是一个等距同构：

$$\| P-Q \| = \| \varphi(\varphi^{-1}(P)) - \varphi(\varphi^{-1}(Q)) \| = \| \varphi^{-1}(P) - \varphi^{-1}(Q) \|.$$

因此，**Isom**$(\mathbb{R}^2)$是一个群，因为由引理 2.6 知，函数的合成总是满足结合律.

读者可以用这个方法证明 $O(2, \mathbb{R})$也是一个群. ■

推论 2.62 *若 O，P，Q 是不共线的点，且 φ 和 ψ 是平面的满足 $\varphi(P)=\psi(P)$和 $\varphi(Q)=\psi(Q)$的等距同构，则 $\varphi=\psi$.*

证明 因为 O，P，Q 不共线，所以在向量空间$\mathbb{R}^2$ 中，P，Q 是线性无关的. 因为 $\dim(\mathbb{R}^2)=2$，所以它是一个基[见推论 4.24(ii)]，而两个线性变换对基的作用一样，所以这两个线性变换相等(见推论 4.63). ■

让我们回到对称性上来.

例 2.63 若△是一个三角形，顶点为 P，Q，U，且 φ 是一个等距同构，则由命题 2.58 知，$\varphi(\triangle)$是一个三角形，顶点为 $\varphi(P)$，$\varphi(Q)$，$\varphi(U)$. 若我们进一步假设 $\varphi(\triangle)=\triangle$，则 φ 置换顶点 P，Q，U(见图 2-13). 假设△的中心是 O. 若△是等腰三角形(腰为 PQ 和 PU)，且 ρ_ℓ是关于轴 $\ell=L[O, P]$的反射，则 $\rho_\ell(\triangle)=\triangle$. (我们可以用对换$(Q\ U)$来描述 ρ_ℓ，因为它固定 P 且交换 Q 和 U). 另一方面，若△不是等腰三角形，则 $\rho_{\ell'}(\triangle)\neq\triangle$，其中 $\ell'=L[O, Q]$. 若△是等边三角形，则 $\rho_{\ell'}(\triangle)=\triangle$，$\rho_{\ell''}(\triangle)=\triangle$，其中 $\ell''=L[O, U]$[我们可以把这些反射分别描述成对换$(P\ U)$和$(P\ Q)$]. 当△只是等腰三角形时，这些反射没有把△变为自身. 另外，关于 O 的 120°和 240°旋转也把△变为自身[这些旋转可以被描述成 3-循环置换$(P\ Q\ U)$和$(P\ U\ Q)$]. 我们看到，等边三角形比等腰三角形“更对称”，等腰三角形比一般的三角形“更对称”[对于这样的三角形，由 $\varphi(\triangle)=\triangle$可得 $\varphi=1$]. ◀ 142

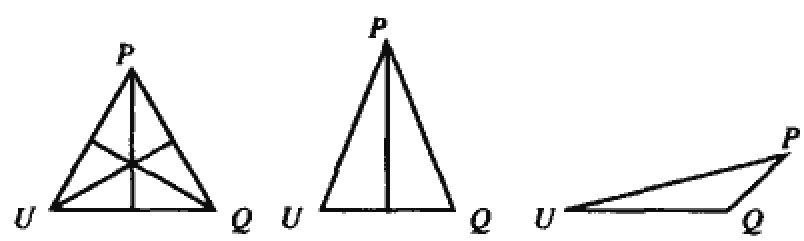


图 2-13　等边三角形，等腰三角形，不等边三角形

→ **定义** 平面上图形 Ω 的**对称群**$\Sigma(\Omega)$是指平面的满足 $\varphi(\Omega)=\Omega$ 的所有等距同构构成的集合. $\Sigma(\Omega)$的元素称为 Ω 的**对称**.

显然，$\Sigma(\Omega)$总是一个群.

例 2.64 (i)正如我们在例 2.63 中所看到的一样，正 3 边形 π_3 是等边三角形，且 $|\Sigma(\pi_3)|=6$.

(ii)设 π_4 是一个正方形(正四边形，如图 2-14 所示)，顶点为$\{v_0, v_1, v_2, v_3\}$. 在平面中画出 π_4，使得它的中心在原点 O，它的边与坐标轴平行. 容易看出，每个 $\varphi\in\Sigma(\pi_4)$置换顶点. 事实上，π_4 的一个对称 φ 由$\{\varphi(v_i): 0\leqslant i\leqslant 3\}$所确定，所以 π_4 至多可能有 $24=4!$ 个对称. 若 v_i 和 v_j 相邻，则 $\|v_i-v_j\|=1$，但是 $\|v_0-v_2\|=\sqrt{2}=\|v_1-v_3\|$，于是 φ 一定保相邻性(因为等距同构保距). π_4 只有 8 个对称(这将在定理 2.65 中证明). 除了恒等函数和关于原点 O 的 90°，180°，270°三个旋转外，还有四个反射，其轴分别为 $L[v_0, v_2]$，$L[v_1, v_3]$， 143

x 轴，y 轴．群 $\Sigma(\pi_4)$ 称为有八个元素的**二面体群**，并记为 D_8．

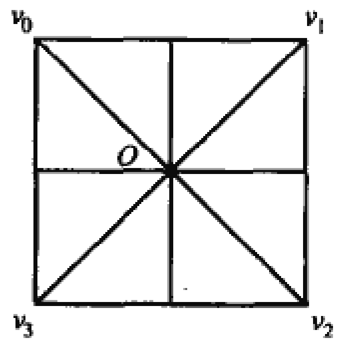


图 2-14 π_4 的对称

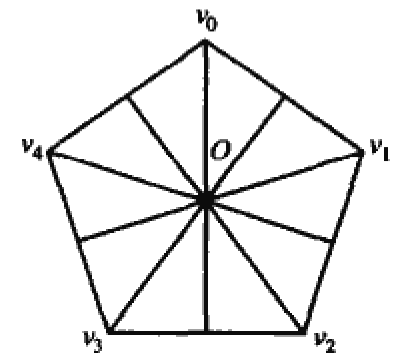


图 2-15 π_5 的对称

(iii)设 π_5 是顶点为 v_0，…，v_4 且中心为 O 的正五边形(如图 2-15)，则 π_5 的对称群 $\Sigma(\pi_5)$ 有 10 个元素：绕原点 $(72j)°$ 的旋转，其中 $0\leqslant j\leqslant 4$，以及轴为 $L[O, v_k]$ 的反射，$0\leqslant k\leqslant 4$(定理 2.65 表明不存在其他的对称了)．对称群 $\Sigma(\pi_5)$ 称为有 10 个元素的**二面体群**，记为 D_{10}．

◀

设 π_n 是顶点为 v_0，v_1，…，v_{n-1} 且中心为 O 的正多边形，则 π_n 的对称群 $\Sigma(\pi_n)$ 称为**二面体群**[⊖]，记为 D_{2n}．下面我们给出一个不依赖于等距同构的定义．

→ **定义** *恰有 $2n$ 个元素的群 D_{2n} 称为*__二面体群__*，若它含有一个阶为 n 的元素 a 和一个阶为 2 的元素 b，且满足 $bab=a^{-1}$．*

若 $n=2$，则二面体群 D_4 是阿贝尔群．若 $n\geqslant 3$，则 D_{2n} 不是阿贝尔群．习题 2.72 表明，实际上只存在一个含 $2n$ 个元素的二面体群(准确地说，任意两个这样的二面体群同构)．

144 → **定理 2.65** *正 n 多边形 π_n 的对称群 $\Sigma(\pi_n)$ 是一个含 $2n$ 个元素的二面体群．*

证明 设 π_n 的顶点为 v_0，v_1，…，v_{n-1}，中心为 O．定义 a 为绕 O 的 $(360/n)°$ 旋转：

$$a(v_i)=\begin{cases}v_{i+1}, & 若\ 0\leqslant i<n-1\\ v_0, & 若\ i=n-1.\end{cases}$$

显然 a 的阶为 n．定义 b 为轴为 $L[O, v_0]$ 的反射，则

$$b(v_i)=\begin{cases}v_0, & 若\ i=0\\ v_{n-i}, & 若\ 1\leqslant i\leqslant n-1.\end{cases}$$

显然 b 的阶为 2．存在 n 个不同的对称 1，a，a^2，…，a^{n-1}(因为 a 的阶为 n)，且 b，ab，a^2b，…，$a^{n-1}b$ 也是各不相同的(根据消去律)．若 $a^s=a^rb$，其中 $0\leqslant r\leqslant n-1$，$s=0$，1，则对所有 i 有 $a^s(v_i)=a^rb(v_i)$．现在 $a^s(v_0)=v_s$，而 $a^rb(v_0)=v_{r-1}$，因而 $s=r-1$．若 $i=1$，则 $a^{r-1}(v_1)=v_{r+1}$，而 $a^rb(v_1)=v_{r-1}$．因此，对所有 r，s 有 $a^s\neq a^rb$，且我们已经展示了 $\Sigma(\pi_n)$ 中的 $2n$ 个不相同的对称．

我们现在证明 π_n 没有其他的对称．我们可以假设 π_n 的中心 O 在原点处，从而每个对称 φ 都固定 O，即 φ 是一个线性变换(根据命题 2.59)．与 v_0 相邻的顶点 v_1 和 v_{n-1} 是与 v_0 最靠近

⊖ 克莱茵(F. Klein)专门研究那些有限群，它们是 $\mathbb{R}^3$ 的等距同构构成的群的子群．其中有一些是正多面体的对称群．他发现了一个退化的多面体，称之为二面体，是由两个全等的零厚度正多边形粘贴在一起构成的．因此一个二面体的对称群称为二面体群．

的顶点，即若 $2\leqslant i\leqslant n-2$，则 $\| v_i-v_0 \| > \| v_1-v_0 \|$. 因此，若 $\varphi(v_0)=v_j$，则 $\varphi(v_1)=v_{j+1}$ 或 $\varphi(v_1)=v_{j-1}$. 在第一种情形中，$a^j(v_0)=\varphi(v_0)$，$a^j(v_1)=\varphi(v_1)$，所以由推论 2.62 知 $\varphi=a^j$. 在第二种情形中，$a^jb(v_0)=v_j$，$a^jb(v_1)=v_{j-1}$，由推论 2.62 知 $\varphi=a^jb$. 因此 $|\Sigma(\pi_n)|=2n$.

我们已经证明了 $\Sigma(\pi_n)$ 是仅有 $2n$ 个元素的群，且含有阶为 n 的元素 a 和阶为 2 的元素 b. 最后只要证明 $bab=a^{-1}$. 由推论 2.62 知，只需计算它们在 v_0 和 v_1 处的值. $bab(v_0)=v_{n-1}=a^{-1}(v_0)$，$bab(v_1)=v_0=a^{-1}(v_1)$，证毕. ■

对称是在微积分中描述平面中的图形时产生的. 我们引用爱德华兹(Edwards)和佩妮(Penny)编著的《微积分与解析几何》(Calculus and Analytic Geometry)，1990 年，第三版，第 456 页. 书中描述了不同类型的对称，这些可能是关于曲线 $f(x, y)=0$ 的对称.

(i)关于 x 轴的对称：当 y 替换为 $-y$ 时曲线的方程不变.

(ii)关于 y 轴的对称：当 x 替换为 $-x$ 时曲线的方程不变.

(iii)关于原点的对称：当 x 替换为 $-x$ 且 y 替换为 $-y$ 时曲线的方程不变.

(iv)关于直线 $y=x$ 的对称：当 x 和 y 互换时方程不变. 145

用我们的话说，第一个对称是 ρ_x，即轴为 x 轴的反射，第二个是 ρ_y，即轴为 y 轴的反射，第三个是 R_{180}，即 180°的旋转，第四个是 ρ_L，其中 L 是 45°直线. 我们现在可以判断含两个变量的方程什么时候具有对称性. 例如，若 $f(x, y)=f(x, -y)$，则函数 $f(x, y)$ 有第一种类型的对称性. 此时，方程 $f(x, y)=0$ 的图像 Γ[由满足 $f(a, b)=0$ 的所有点 (a, b) 构成]关于 x 轴对称，这是因为由 $(a, b)\in\Gamma$ 可推出 $(a, -b)\in\Gamma$.

习题

H 2.36 判断对错并说明理由.

(i)函数 e: $\mathbf{N}\times\mathbf{N}\to\mathbf{N}$，$e(m, n)=m^n$，满足结合律.

(ii)每个群都是 Abel 群.

(iii)所有正实数构成的集合对乘法作成群.

(iv)所有正实数构成的集合对加法作成群.

(v)对所有 $a, b\in G$，其中 G 是一个群，有 $aba^{-1}b^{-1}=1$.

(vi)顶点为 v_1，v_2，v_3 的等边三角形 π_3 的每个置换是 π_3 的对称的限制.

(vii)顶点为 v_1，v_2，v_3，v_4 的正方形 π_4 的每个置换是 π_4 的对称的限制.

(viii)$a, b\in G$，其中 G 是一个群，则对所有 $n\in\mathbf{N}$ 有 $(ab)^n=a^nb^n$.

(ix)每个无限群都含有一个阶为无限的元素.

(x)复共轭置换每个实系数多项式的根.

2.37 若 $a_1, a_2, \cdots, a_n$ 是群 G 中的元素(不必互不相同)，证明

$$(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}.$$

2.38 (i)求 $\alpha=(1\ 2)(4\ 3)(1\ 3\ 5\ 4\ 2)(1\ 5)(1\ 3)(2\ 3)$ 的阶、逆元和奇偶性.

(ii)习题 2.22 和 2.28 中的置换的阶各是多少?

2.39 H (i)S_5 和 S_6 中阶为 2 的元素有多少个?

H (ii)S_n 中阶为 2 的元素有多少个?

*H 2.40 设 G 是一个群，$y\in G$ 的阶为 m. 若存在 $d\geqslant 1$ 使得 $m=dt$，证明 y^t 的阶为 d.

*2.41 设 G 是一个群，$a\in G$ 的阶为 dk，其中 $d, k>1$. 证明，若存在 $x\in G$ 使得 $x^d=a$，则 x 的阶为 d^2k. 由

146 此知 x 的阶比 a 的阶大.

2.42 设 $G=GL(2,\mathbb{Q})$，并设 $A=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$和 $B=\begin{bmatrix}0 & 1\\ -1 & 1\end{bmatrix}$. 证明，$A^4=I=B^6$，但对所有 $n>0$ 有$(AB)^n\neq I$. 由此得，即使因子 A 和 B 都有有限阶，AB 也可能有无限阶(这在有限群中是不可能发生的).

2.43 H (i)对 $k\geqslant 1$ 用归纳法证明

$$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}^k=\begin{bmatrix}\cos k\theta & -\sin k\theta\\ \sin k\theta & \cos k\theta\end{bmatrix}.$$

(ii)求出特殊正交群 $SO(2,\mathbb{R})$[见例 2.48(iii)]中阶有限的所有元素.

*2.44 设 G 是一个群，满足对每个 $x\in G$ 有 $x^2=1$，证明 G 是阿贝尔群. [例 2.47(viii)中的布尔群$B(X)$就是这样的群.]

*H 2.45 设 G 是一个有限群，其每个元素都有一个平方根，即对每个 $x\in G$，存在 $y\in G$ 满足 $y^2=x$. 证明 G 中每个元素都有唯一的平方根.

*H 2.46 若 G 是一个群，其元素个数为偶数，证明 G 中阶为 2 的元素个数是奇数. 特别地，G 一定含有阶为 2 的元素.

H 2.47 在 S_n 中元素的最大阶是多少，其中 $n=1, 2, \cdots, 10$?

*2.48 随机[⊖]群$\Sigma(2,\mathbb{R})$是由 $GL(2,\mathbb{R})$中列和为 1 的矩阵构成的，即$\Sigma(2,\mathbb{R})$是由所有非奇异矩阵 $\begin{bmatrix}a & c\\ b & d\end{bmatrix}$构成的，其中 $a+b=1=c+d$. [也有随机群$\Sigma(2,\mathbb{Q})$和$\Sigma(2,\mathbb{C})$.]

证明两个随机矩阵的积仍是一个随机矩阵，一个随机矩阵的逆仍是随机矩阵.

2.49 证明圆 C 的对称群$\Sigma(C)$是无限群.

*2.50 证明，在二面体群 D_{2n}中，每个元素有形如 a^ib^j 的唯一分解，其中 $0\leqslant i<n$，$j=0$ 或 1.

2.51 设 $e_1=(1,0)$，$e_2=(0,1)$. 若 φ 是平面的固定 O 的等距同构，设 $\varphi(e_1)=(a,b)$，$\varphi(e_2)=(c,d)$，$A=\begin{bmatrix}a & c\\ b & d\end{bmatrix}$，证明 $\det(A)=\pm 1$.

→2.4 子群和拉格朗日定理

群 G 的子群是 G 的子集，它在 G 的运算下构成一个群. 下面的定义使后面这句话更准确.

→ **定义** 设 $*$ 是集合 G 上的运算，$S\subseteq G$ 是子集. 我们说 S **在 $*$ 下封闭**，若对所有 $x, y\in S$ 有 $x*y\in S$.

群 G 上的运算是函数 $*: G\times G\to G$. 若 $S\subseteq G$，则 $S\times S\subseteq G\times G$. S 在 $*$ 下封闭是指 $*(S\times S)\subseteq S$. 例如，加法群$\mathbb{Q}$ 的子集$\mathbb{Z}$ 在$+$下封闭. 若$\mathbb{Q}^\times$是非零有理数构成的乘法群，则 $\mathbb{Q}^\times$在乘法下封闭，但是它在$+$下不封闭(例如，2 和-2 属于$\mathbb{Q}^\times$，但是它们的和$-2+2=$

147 $0\notin\mathbb{Q}^\times$).

→ **定义** 群 G 的子集 H 称为**子群**，若

(i)$1\in H$;

(ii)若 $x, y\in H$，则 $xy\in H$；即 H 在 $*$ 下封闭；

⊖ 术语"随机的(stochastic)"来自意思为"猜测"的希腊词. 它的数学用法最早出现在统计学中. 随机矩阵首次出现在对某些随机问题的研究中.

(iii)若 $x\in H$，则 $x^{-1}\in H$.

我们用 $H\leqslant G$ 表示 H 是群 G 的子群. 观察到，$\{1\}$ 和 G 总是群 G 的子群，其中 $\{1\}$ 表示由单一的元素 1 构成的子集. 我们称 G 的子群 H 是**真子群**，若 $H\neq G$，并记为 $H<G$. 我们称 G 的子群 H 是**非平凡的**，若 $H\neq\{1\}$. 下面将给出更有趣的例子.

→ **命题 2.66** *群 G 的每个子群 $H\leqslant G$ 本身是一个群.*

证明 公理(ii)(在子群的定义中)表明 H 在 G 的运算下封闭，即 H 有一个运算(本质上，它是运算 $*: G\times G\to G$ 对 $H\times H\subseteq G\times G$ 的限制). 这个运算满足结合律：因为等式 $(xy)z=x(yz)$ 对所有 $x, y, z\in G$ 成立，特别地，这个等式对所有 $x, y, z\in H$ 成立. 最后，公理(i)给出单位元，公理(iii)给出逆元. ■

验证群 G 的子集 H 是一个子群(因而它本身是一个群)比验证 H 满足群公理更快，因为结合律是从 G 上的运算继承来的，因而不须再验证了.

→ **例 2.67** (i)回忆 $\mathbf{Isom}(\mathbb{R}^2)$ 是平面的所有等距同构构成的群. 子集 $O(2, \mathbb{R})$ 是由所有固定原点的等距同构构成的，是 $\mathbf{Isom}(\mathbb{R}^2)$ 的一个子群. 若 $\Omega\subseteq\mathbb{R}^2$，则对称群 $\Sigma(\Omega)$ 也是 $\mathbf{Isom}(\mathbb{R}^2)$ 的一个子群. 若 Ω 的重心存在且在原点处，则 $\Sigma(\Omega)\leqslant O(2, \mathbb{R})$.

(ii)这四个置换

$$\mathbf{V}=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$

构成一个群，因为 $\mathbf{V}$ 是 S_4 的一个子群：$(1)\in\mathbf{V}$；对任意 $\alpha\in\mathbf{V}$ 有 $\alpha^2=(1)$，因而 $\alpha^{-1}=\alpha\in\mathbf{V}$；$\mathbf{V}-\{(1)\}$ 中任意两个不同置换的乘积是第三个元素. 我们称 $\mathbf{V}$ 是**四元群(或克莱因(Klein)群)**($\mathbf{V}$ 是德语 Vierergruppe 的缩写).

考虑验证结合律 $a(bc)=(ab)c$ 需要做什么：a，b，c 中每一个都有四种选法，所以共 $4^3=64$ 个等式要验证. 当然，我们可以假设它们中没有(1)，则剩下 $3^3=27$ 个等式要验证. 显然，利用验证 $\mathbf{V}$ 是 S_4 的子群去证明 $\mathbf{V}$ 是群更简单. 148

(iii)若把平面 $\mathbb{R}^2$ 看作是一个(加法)阿贝尔群，则过原点的任意直线 L 是它的子群. 为看出这一点，最简单的办法是取 L 上的一个非零点 (a, b)，并注意 L 是由所有纯量倍数 (ra, rb) 构成的. 读者可以验证 L 满足子群定义中的三个公理. ◀

实际上我们可以简化子集是子群所需要的三个条件.

→ **命题 2.68** *群 G 的子集 H 是一个子群当且仅当 H 非空，且对任意 $x, y\in H$ 有 $xy^{-1}\in H$.*

证明 若 H 是一个子群，因为 $1\in H$，所以 H 非空. 设任意 $x, y\in H$，由子群定义中的公理(iii)知 $y^{-1}\in H$，又由公理(ii)知 $xy^{-1}\in H$.

反之，假设子集 H 满足新的条件. 因为 H 非空，所以它含有某个元素，不妨设为 h. 取 $x=h=y$，则 $1=hh^{-1}\in H$，因此公理(i)成立. 若 $y\in H$，则令 $x=1$(因为 $1\in H$，所以能这样做)，得 $y^{-1}=1y^{-1}\in H$，所以定义中的公理(iii)成立. 最后，由引理 2.46 知 $(y^{-1})^{-1}=y$. 因此，若 $x, y\in H$，则 $y^{-1}\in H$，所以 $xy=x(y^{-1})^{-1}\in H$. 因此，H 是 G 的子群. ■

因为每个子群含有 1，所以我们可以在命题 2.68 中用“$1\in H$”替换“H 非空”.

注意，若群 G 中的运算是加法，则命题中的条件是：H 是非空子集且对任意 $x, y\in H$ 有 $x-y\in H$.

伽罗瓦提出：若 S_n 的子集 H 在合成运算下封闭，即，若 α，$\beta\in H$，则 $\alpha\beta\in H$，则 H 是群. 1854 年，凯莱(A. Cayley)第一个定义了抽象群的概念并明确提到了结合律、逆元和单位元的概念.

命题 2.69 *有限群 G 的非空子集 H 是一个子群当且仅当 H 在 G 的运算下封闭，即，若 a，$b\in H$，则 $ab\in H$. 特别地，S_n 的非空子集是子群当且仅当它在合成运算下封闭.*

证明 由子群定义中的公理(i)知每个子群是非空的，由公理(ii)知它在 G 的运算下是封闭的.

反之，假设 H 是 G 的非空子集，且在 G 的运算下封闭，则公理(ii)成立. 于是 H 包含它的元素的所有幂. 特别地，因为 H 是非空的，所以存在 $a\in H$，并且对所有 $n\geqslant 1$ 有 $a^n\in H$. 像在例 2.52 中看到的一样，G 中每个元素都有有限阶：存在整数 m 使得 $a^m=1$. 因此 $1\in H$，(i)成立. 最后，若 $h\in H$，$h^m=1$，则 $h^{-1}=h^{m-1}$(因为 $hh^{m-1}=1=h^{m-1}h$)，所以 $h^{-1}\in H$，(iii)成立. 因此，H 是 G 的子群. ■

当 G 是无限群时，命题 2.69 可能是错误的. 例如，加法群 $\mathbb{Z}$ 的子集 $\mathbb{N}$ 在 $+$ 下封闭，但它
149 不是 $\mathbb{Z}$ 的子群.

例 2.70 S_n 的子集 $A_n=\{$所有的偶置换$\}$是一个子群，因为它在乘法下封闭：偶∘偶=偶. S_n 的这个子群称为 n 次**交错**[⊖]群，并记为 A_n. ◀

定义 设 G 是一个群，$a\in G$，记

$$\langle a\rangle=\{a^n:n\in\mathbb{Z}\}=\{a\text{ 的所有幂}\},$$

则 $\langle a\rangle$ 称为由 a **生成的** G **的循环子群**.

群 G 称为**循环群**，如果存在 $a\in G$ 使得 $G=\langle a\rangle$，此时称 a 为 G 的**生成元**.

易知 $\langle a\rangle$ 实际上是一个子群：$1=a^0\in\langle a\rangle$；$a^na^m=a^{n+m}\in\langle a\rangle$；$a^{-1}\in\langle a\rangle$. 由例 2.47(v)知，对每个 $n\geqslant 1$，由所有 n 次单位根构成的乘法群 Γ_n 是循环群，其生成元是 n 次本原单位根 $\zeta=e^{2\pi i/n}$.

循环群可能有几个不同的生成元. 例如，$\langle a\rangle=\langle a^{-1}\rangle$. 若 $(k,n)=1$，则 n 次本原单位根 $e^{2\pi ik/n}$ 也是 Γ_n 的生成元.

命题 2.71 *设 $G=\langle a\rangle$ 是一个阶为 n 的循环群，则 a^k 是 G 的生成元当且仅当 $\gcd(k,n)=1$.*

证明 若 a^k 是生成元，则 $a\in\langle a^k\rangle$，所以存在 s 使得 $a=a^{ks}$. 因而 $a^{ks-1}=1$，由引理 2.53 知 $n\mid(ks-1)$，即，存在一个整数 t 使得 $ks-1=tn$，或 $sk-tn=1$. 因而由习题 1.56 知 $(k,n)=1$.

反之，因为 $\gcd(k,n)=1$，所以存在整数 s 和 t 使得 $1=sk+tn$. 因而 $a=a^{sk+tn}=a^{sk}$(因为 $a^n=1$)，所以 $a\in\langle a^k\rangle$. 因此 $G=\langle a\rangle\leqslant\langle a^k\rangle$，所以 $G=\langle a^k\rangle$. ■

推论 2.72 *阶为 n 的循环群有 $\phi(n)$ 个生成元.*

⊖ 交错群是在研究多项式时产生的. 若 $f(x)=(x-u_1)(x-u_2)\cdots(x-u_n)$，则当我们置换它的根时，数 $D=\prod_{i<j}(u_i-u_j)$ 会改变符号：若 α 是 $\{u_1,u_2,\cdots,u_n\}$ 的一个置换，则容易看出 $\prod_{i<j}[\alpha(u_i)-\alpha(u_j)]=\pm D$. 因此，当不同的置换 α 作用因子时，积的符号交替变化. 若 α 是交错群中的元素，则符号不改变.

证明 由命题 2.71 和命题 1.42 立即可得. ■ 150

→ **命题 2.73** 循环群 $G=\langle a\rangle$ 的每个子群 S 本身是一个循环群. 实际上, a^k 是 S 的生成元, 其中 k 是使 $a^m\in S$ 的最小正整数 m.

证明 我们可以假设 S 是非平凡的, 即 $S\neq\{1\}$, 因为当 $S=\{1\}$ 时命题显然成立. 设 $I=\{m\in\mathbb{Z}: a^m\in S\}$. 我们验证 I 满足推论 1.37 中的三个条件. 首先, $0\in I$, 因为 $a^0=1\in S$. 其次, 若 $m, n\in I$, 则 $a^m, a^n\in S$, 所以 $a^m a^{-n}=a^{m-n}\in S$, 因而 $m-n\in I$. 第三, 若 $m\in I$, $i\in\mathbb{Z}$, 则 $a^m\in S$, 所以 $(a^m)^i=a^{im}\in S$, 因而 $im\in I$. 因为 $S\neq\{1\}$, 所以存在某个 $a^q\in S$ 使 $a^q\neq 1$. 因此 $q\in I$, $I\neq\{0\}$. 根据推论 1.37, $I=(k)$, 其中 k 是 I 中的最小正整数, 所以对每个 $m\in I$ 有 $k\mid m$. 我们断言 $\langle a^k\rangle=S$. 显然, $\langle a^k\rangle\leqslant S$. 对于反包含, 取 $s\in S$. 现在对某个 m 有 $s=a^m$, 所以 $m\in I$ 且对某个 ℓ 有 $m=k\ell$. 因此 $s=a^m=a^{k\ell}\in\langle a^k\rangle$. ■

命题 2.80 将对命题 2.73 给出数论方面的解释.

→ **命题 2.74** 设 G 是一个有限群, 且 $a\in G$, 则 a 的阶等于 $\langle a\rangle$ 中元素的个数.

证明 我们将应用引理 2.23 中的思想. 因为 G 是有限的, 所以存在整数 $k\geqslant 1$ 使得 $1, a, a^2, \cdots, a^{k-1}$ 是 G 中 k 个不同的元素, 而 $1, a, a^2, \cdots, a^k$ 出现重复. 因此 $a^k\in\{1, a, a^2, \cdots, a^{k-1}\}$, 即, 对某个 i, $0\leqslant i<k$, 有 $a^k=a^i$. 若 $i\geqslant 1$, 则 $a^{k-i}=1$, 此与 $1, a, a^2, \cdots, a^{k-1}$ 无重复矛盾. 因此, $a^k=a^0=1$, k 是 a 的阶(因为 k 是这样的最小正整数).

设 $H=\{1, a, a^2, \cdots, a^{k-1}\}$, 则 $|H|=k$, 只须证明 $H=\langle a\rangle$. 显然, $H\subseteq\langle a\rangle$. 对于反包含, 取 $a^i\in\langle a\rangle$. 由除法算式知 $i=qk+r$, 其中 $0\leqslant r<k$. 因此 $a^i=a^{qk+r}=a^{qk}a^r=(a^k)^q a^r=a^r\in H$, 由此得 $\langle a\rangle\subseteq H$. 所以 $H=\langle a\rangle$. ■

→ **定义** 设 G 是一个有限群, G 中元素的个数称为 G 的阶, 记为 $|G|$.

"阶"在群论中有两种含义: 元素 $a\in G$ 的阶和群 G 的阶 $|G|$. 由命题 2.74 知, 群元素 a 的阶等于 $|\langle a\rangle|$.

有限循环群的下述特征将用来证明定理 3.55, 说明有限域的乘法群是循环群.

→ **命题 2.75** 设 G 是一个阶为 n 的群. 若 G 是循环群, 则对 n 的每个因子 d, G 有唯一的阶为 d 的子群. 反之, 若至多存在一个阶为 d 的循环子群, 其中 $d\mid n$, 则 G 是循环群. 151

证明 假设 $G=\langle a\rangle$ 是阶为 n 的循环群. 我们断言, $\langle a^{n/d}\rangle$ 的阶为 d. 显然, $(a^{n/d})^d=a^n=1$, 所以只须证明 d 是这样的最小正整数. 若 $(a^{n/d})^r=1$, 则由引理 2.53 知, $n\mid(n/d)r$. 因而存在整数 s 满足 $(n/d)r=ns$, 这样 $r=ds$, $r\geqslant d$.

为证明唯一性, 设 C 是 G 的阶为 d 的子群. 由命题 2.73 知, 子群 C 是循环群, 不妨设 $C=\langle x\rangle$. 现在 $x=a^m$ 的阶为 d, 所以 $1=(x^m)^d$. 因而由引理 2.53 知 $n\mid md$, 所以 $md=nk$, k 为整数. 因此, $x=a^m=(a^{n/d})^k$, 所以 $C=\langle x\rangle\subseteq\langle a^{n/d}\rangle$. 因为两个子群的阶相同, 所以 $C=\langle a^{n/d}\rangle$.

反之, 定义群 G 上的一个关系 $a\equiv b$, 若 $\langle a\rangle=\langle b\rangle$. 容易看出, 这是一个等价关系, 且 $a\in G$ 的等价类 $[a]$ 由 $C=\langle a\rangle$ 的所有生成元构成. 因此, 我们用 $\text{gen}(C)$ 表示 $[a]$, 且

$$G=\bigcup_{C\text{是循环群}}\text{gen}(C).$$

因而 $n=|G|=\sum_C|\text{gen}(C)|$. 由推论 2.72 知 $|\text{gen}(C)|=\phi(|C|)$. 根据假设, G 至多

有一个任意阶的循环子群，所以

$$n=\sum_{C}|\operatorname{gen}(C)|\leqslant\sum_{d\mid n}\phi(d)=n,$$

最后一个等式就是推论 1.31. 因此，对 n 的每个因子 d，一定存在阶为 d 的循环子群 C，分配 $\phi(d)$ 给 $\sum_{C}|\operatorname{gen}(C)|$. 特别地，一定存在阶为 n 的循环子群 C，所以 G 是循环群. ■

下面是从已知群构造新群的一种方法.

→ **命题 2.76** *群 G 的任一族子群的交 $\bigcap_{i\in I}H_i$ 还是 G 的子群. 特别地，若 H，K 都是 G 的子群，则 $H\cap K$ 也是 G 的子群.*

证明 令 $D=\bigcap_{i\in I}H_i$，我们通过验证子群定义的各部分来证明 D 是一个子群. 首先注意到 $D\neq\varnothing$，因为对所有 i 有 $1\in H_i$，所以 $1\in D$. 假设 $x\in D$，则 $x\in H_i$，因为每个 H_i 都是子群，所以对所有 i 有 $x^{-1}\in H_i$，所以 $x^{-1}\in D$. 最后，若 x，$y\in D$，则对所有 i 有 x，$y\in H_i$，因此 $xy\in H_i$，所以 $xy\in D$. ■

→ **推论 2.77** *设 X 是群 G 的一个子集，则存在 G 的包含 X 的一个最小子群 $\langle X\rangle$，即，对 G*
152 *的包含 X 的每个子群 H 都有 $\langle X\rangle\leqslant H$.*

证明 首先我们注意到，G 的包含 X 的子群存在，例如，G 本身包含 X. 定义 $\langle X\rangle=\bigcap_{X\subseteq H}H$，是 G 的所有包含 X 的子群 H 的交集. 由命题 2.76 知，$\langle X\rangle$ 是 G 的一个子群. 因为每个 H 包含 X，所以 $\langle X\rangle$ 也包含 X. 最后，若 H 是任意一个包含 X 的子群，则 H 是交集为 $\langle X\rangle$ 的子群族中的一个，所以 $\langle X\rangle\leqslant H$. ■

注意 *在推论 2.77 中对子集 X 没有任何限制. 特别地，$X=\varnothing$ 是允许的. 因为空集是任何集合的子集，所以对 G 的每个子群 H 都有 $\varnothing\subseteq H$. 这样，$\langle\varnothing\rangle$ 是 G 的所有子群的交，其中一个是 $\{1\}$，所以 $\langle\varnothing\rangle=\{1\}$.*

→ **定义** *若 X 是群 G 的一个子集，则 $\langle X\rangle$ 称为由 **X 生成的子群**.*

例 2.78 (i)若 $G=\langle a\rangle$ 是由 a 生成的循环群，则 G 是由子集 $X=\{a\}$ 生成的. 但是，我们总是写 $\langle a\rangle$，而不写 $\langle\{a\}\rangle$.

(ii)正 n 边形 π_n 的对称群 $\Sigma(\pi_n)$ 是由 a，b 生成的，其中 a 是绕原点 $(360/n)^\circ$ 的旋转，b 是一个反射(见定理 2.65). 这些生成元满足条件 $a^n=1$，$b^2=1$ 和 $bab=a^{-1}$，且 $\Sigma(\pi_n)$ 是一个二面体群 D_{2n}. ◀

下面的命题更具体地描述了由子集生成的子群.

定义 *设 X 是群 G 的子集，则 X 上的**字**是指单位元或 G 的形如 $\omega=x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ 的元素，其中 $n\geqslant1$，对所有 i 有 $x_i\in X$，且 $e_i=\pm1$.*

命题 2.79 *若 X 是群 G 的子集，则 $\langle X\rangle$ 是由 X 上的所有字构成的集合.*

证明 我们先证明由 X 上的所有字构成的集合 W 是 G 的子群. 根据定义，$1\in W$，即使 $X=\varnothing$. 若 w，$w'\in W$，则 $w=x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$，$w'=y_1^{f_1}y_2^{f_2}\cdots y_m^{f_m}$，其中 x_i，$y_j\in X$，e_i，$f_j=\pm1$. 因此 $ww'=x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}y_1^{f_1}y_2^{f_2}\cdots y_m^{f_m}$，它是 X 上的字，所以 $ww'\in W$. 最后，$(w)^{-1}=x_n^{-e_n}x_{n-1}^{-e_{n-1}}\cdots x_1^{-e_1}\in W$. 因此 W 是 G 的子群，它显然含有 X 的每个元素，所以 $\langle X\rangle\leqslant W$. 对于

相反的不等式，我们证明，若 S 是 G 的包含 X 的任意子群，则 S 包含 X 上的任意字．但是，这是显然的：因为 S 是一个子群，所以只要 $x\in X$ 和 $e=\pm 1$ 它就含有 x^e，且它含有这种元素的所有可能积．因此，对所有这样的 S 有 $W\leqslant S$，所以 $W\leqslant\bigcap_S=\langle X\rangle$． ■ 153

命题 2.80　*设 a，b 都是整数，并设 $A=\langle a\rangle$，$B=\langle b\rangle$ 是 $\mathbb{Z}$ 的分别由 a，b 生成的循环子群．*

(i)若 $A+B$ 定义为 $\{sa+tb: s, t\in\mathbb{Z}\}$，则 $A+B=\langle d\rangle$，其中 $d=\gcd(a, b)$．

(ii)$A\cap B=\langle m\rangle$，其中 $m=\text{lcm}(a, b)$．

证明　(i)在加法中，字正是一个线性组合，所以由命题 2.79 知，$A+B$ 是 $\mathbb{Z}$ 的由 $A\cup B$ 生成的子群．根据命题 2.73，$A+B$ 是循环群，所以 $A+B=\langle d\rangle$，其中 d 是 a 和 b 的最小非负线性组合．因此，由定理 1.35 的证明知 $d=\gcd(a, b)$．

(ii)若 $c\in A\cap B$，则 $c\in A$ 且 $a\mid c$．类似地有 $c\in B$ 且 $b\mid c$．因此，$A\cap B$ 中每个元素是 a 和 b 的公倍数．反之，每个公倍数都在 $A\cap B$ 中．根据命题 2.73，子群 $A\cap B$ 是循环群：$A\cap B=\langle m\rangle$，其中 m 可选为 $A\cap B$ 中最小的非负整数．因此，m 是最小公倍数，即 $m=\text{lcm}(a, b)$． ■

对于有限群 G 的子群 H，有一个最基本的事实：H 的阶是受限制的．当然，我们有 $|H|\leqslant|G|$，但还可以得出 $|H|$ 一定是 $|G|$ 的因子．为证明这一点，我们先介绍陪集的概念．

定义　*若 H 是群 G 的子群且 $a\in G$，则**陪集**[⊖] aH 是指 G 的子集 aH，其中*

$$aH=\{ah: h\in H\}.$$

当然，$a=a1\in aH$．陪集通常不是子群．例如，若 $a\notin H$，则 $1\notin aH$(否则，存在 $h\in H$ 使得 $1=ah$，这与 $a=h^{-1}\in H$ 矛盾)．

如果我们使用群 G 中的运算符号 $*$，则陪集 aH 记为 $a*H$，其中

$$a*H=\{a*h: h\in H\}.$$

特别地，若运算是加法，则陪集记为

$$a+H=\{a+h: h\in H\}.$$ 154

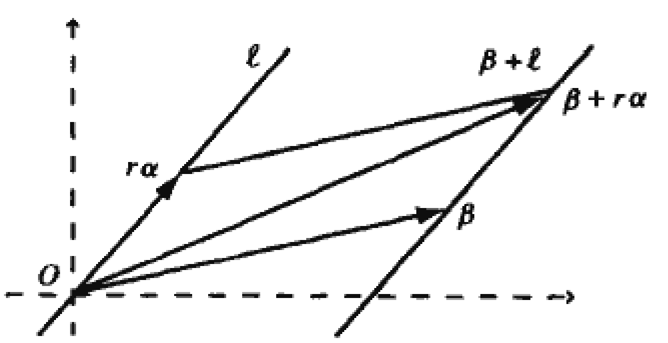


图 2-16　陪集 β+ℓ

例 2.81　(i)把平面 $\mathbb{R}^2$ 看作是(加法)阿贝尔群，令 ℓ 是过原点 O 的直线(见图 2-16)，像例 2.67(iii)一样，直线 ℓ 是 $\mathbb{R}^2$ 的子群．若 $\beta\in\mathbb{R}^2$，则陪集 $\beta+\ell$ 是一条包含 β 且与 ℓ 平行的直线 ℓ'．这是因为，若 $r\alpha\in\ell$，则由平行四边形法则得 $\beta+r\alpha\in\ell'$．

(ii)设 $G=S_3$，$H=\langle(1\,2)\rangle$，则 H 恰有三个陪集，即：

$$H=\{(1),(1\ 2)\}=(1\ 2)H,$$
$$(1\ 3)H=\{(1\ 3),(1\ 2\ 3)\}=(1\ 2\ 3)H,$$
$$(2\ 3)H=\{(2\ 3),(1\ 3\ 2)\}=(1\ 3\ 2)H,$$

⊖ 这里定义的陪集通常称为左陪集．H 也有右陪集，即形如 $Ha=\{ha: h\in H\}$ 的子集．这些概念都是在群的进一步研究中产生的，但是我们现在只需用(左)陪集处理问题．

每个陪集大小均为 2. ◀

在这些例子中，我们观察到给定的子群的不同陪集是不相交的.

设 H 是群 G 的子群，定义 G 上的一个关系：

$$a \equiv b \quad 当且仅当 \quad a^{-1}b \in H.$$

该关系是 G 上的等价关系. 若 $a \in G$，则 $a^{-1}a=1\in H$，所以 $a\equiv a$，因此≡有自反性. 若 $a\equiv b$，则 $a^{-1}b\in H$，因为子群在逆下封闭，所以 $(a^{-1}b)^{-1}=b^{-1}a\in H$，所以 $b\equiv a$，因此≡有对称性. 若 $a\equiv b$ 和 $b\equiv c$，则 $a^{-1}b$，$b^{-1}c\in H$，因为子群在乘法下封闭，所以 $(a^{-1}b)(b^{-1}c)=a^{-1}c\in H$，所以 $a\equiv c$，因此≡有传递性. 因而它是一个等价关系.

我们断言 $a\in H$ 的等价类是陪集 aH. 若 $x\equiv a$，则存在 $h\in H$ 使得 $a^{-1}x=h$. 因而 $x=ah\in aH$，$[a]\subseteq aH$. 对于反包含，容易看出，若 $x=ah\in aH$，则 $x^{-1}a=(ah)^{-1}a=h^{-1}a^{-1}a=h\in$
155 H，所以 $x\equiv a$，$x\in[a]$，因而 $aH\subseteq[a]$. 所以 $[a]=aH$.

引理 2.82 *设 H 是群 G 的子群，a，$b\in G$.*

(i) $aH=bH$ 当且仅当 $b^{-1}a\in H$. 特别地，$aH=H$ 当且仅当 $a\in H$.

(ii) 若 $aH\cap bH\neq\varnothing$，则 $aH=bH$.

(iii) 对所有 $a\in G$ 有 $|aH|=|H|$.

证明 (i) 这是引理 2.19 的特殊情形，因为陪集是等价类. 因为 $H=1H$，所以 $aH=H=1H$ 当且仅当 $a=1^{-1}a\in H$.

(ii) 这是命题 2.20 的特殊情形，因为等价类组成 X 的分类.

(iii) 容易看出，函数 $f: H\to aH$，$f(h)=ah$ 是一个双射[其反函数 $aH\to H$ 由 $ah\mapsto a^{-1}(ah)=h$ 给定]. 因此，根据习题 2.12 知，H 和 aH 有相同的元素个数. ■

→ **定理 2.83(拉格朗日定理)** *若 H 是有限群 G 的一个子群，则 $|H|$ 是 $|G|$ 的一个因子.*

证明 设 $\{a_1H, a_2H, \cdots, a_tH\}$ 是 G 中 H 的所有不同陪集构成的族. H 的陪集划分 G，因为它们都是等价类. 因而

$$G=a_1H\cup a_2H\cup\cdots\cup a_tH.$$

(习题 2.53 要求我们不用等价类直接证明 G 是 H 的陪集的无交并.) 所以

$$|G|=|a_1H|+|a_2H|+\cdots+|a_tH|.$$

由引理 2.82(iii) 知，对所有 i 有 $|a_iH|=|H|$，所以 $|G|=t|H|$. ■

→ **定义** *群 G 的子群 H 的陪集个数称为 H 在 G 中的***指数***，记为 $[G:H]$.*

当 G 是有限群时，指数 $[G:H]$ 就是公式 $|G|=t|H|$ 中的 t，所以

$$|G|=[G:H]|H|.$$

这个公式告诉我们指数 $[G:H]$ 也是 $|G|$ 的因子.

→ **推论 2.84** *若 H 是有限群 G 的子群，则*

$$[G:H]=|G|/|H|.$$

156 **证明** 由拉格朗日定理立即可得. ■

回忆定理 2.65：正 n 边形的对称群 $\Sigma(\pi_n)$ 是一个阶为 $2n$ 的二面体群. 它包含一个由旋转 a 生成的阶为 n 的循环子群，且子群 $\langle a\rangle$ 有指数 $[\Sigma(\pi_n):\langle a\rangle]=2$. 因此，存在两个陪集：$\langle a\rangle$

和 $b\langle a\rangle$，其中 b 是在 $\langle a\rangle$ 之外的任意一个对称.

我们现在明白了为什么表 2-3 中展示的 S_5 的元素的阶都是 120 的因子. 推论 2.146 将解释为什么 S_5 中的任意给定循环结构的置换的个数是 120 的一个因子.

→ **推论 2.85** *若 G 是有限群且 $a\in G$，则 a 的阶整除 $|G|$.*

证明 由命题 2.74 知，a 的阶等于子群 $H=\langle a\rangle$ 的阶. ■

→ **推论 2.86** *若有限群 G 的阶是 m，则对所有 $a\in G$ 有 $a^m=1$.*

证明 由推论 2.85 知，a 的阶 d 满足 $d\mid m$，即，存在整数 k 使 $m=dk$. 因此 $a^m=a^{dk}=(a^d)^k=1$. ■

→ **推论 2.87** *若 p 是素数，则阶为 p 的群 G 都是循环群.*

证明 取 $a\in G$ 满足 $a\neq 1$，并令 $H=\langle a\rangle$ 是由 a 生成的循环子群. 由拉格朗日定理知，$|H|$ 是 $|G|=p$ 的一个因子. 因为 p 是素数且 $|H|>1$，所以 $|H|=p=|G|$，所以 $H=G$. ■

拉格朗日定理是说，有限群 G 的子群的阶是 $|G|$ 的因子. 拉格朗日定理的"逆命题"成立吗？即，若 d 是 $|G|$ 的一个因子，则一定存在 G 的阶为 d 的子群吗？回答是"不一定". 命题 2.99将证明，交错群 A_4 是阶为 12 的群，它没有阶为 6 的子群.

习题

H 2.52 判断对错并说明理由. 这里 G 总是群.

(i)若 H 是 K 的子群且 K 是 G 的子群，则 H 是 G 的子群.

(ii)G 是自身的一个子群.

(iii)空集 $\varnothing$ 是 G 的一个子群.

(iv)若 G 是有限群且 m 是 $|G|$ 的一个因子，则 G 含有阶为 m 的元素.

(v)S_n 的每个子群的阶都整除 $n!$.

(vi)若 H 是 G 的子群，则 H 的两个(左)陪集的交还是 H 的(左)陪集.

(vii)G 的两个循环子群的交还是循环子群. 157

(viii)若 X 是 G 的有限子集，则 $\langle X\rangle$ 是有限子群.

(ix)若 X 是无限集，则

$$F=\{\sigma\in S_X: \sigma \text{ 只移动 } X \text{ 的有限多个元素}\}$$

是 S_X 的子群.

(x)S_3 的每个真子群都是循环群.

(xi)S_4 的每个真子群都是循环群.

*2.53 设 H 是有限群 G 的子群，$a_1H,\cdots,a_tH$ 是 H 在 G 中的所有不同陪集. 不用 G 上的等价关系：$a\equiv b$ 当且仅当 $b^{-1}a\in H$，证明下面的命题：

(i)证明，对每个 $g\in G$ 有 $g\in gH$，且对某个 i 有 $gH=a_iH$. 由此知 $G=a_1H\cup\cdots\cup a_tH$.

(ii)若 $a,b\in G$ 且 $aH\cap bH\neq\varnothing$，证明 $aH=bH$. 由此知，若 $i\neq j$，则 $a_iH\cap a_jH=\varnothing$.

2.54 (i)定义**特殊线性群**为

$$\mathrm{SL}(2,\mathbf{R})=\{A\in \mathrm{GL}(2,\mathbf{R}): \det(A)=1\}.$$

证明 SL(2, **R**)是 GL(2, **R**)的子群.

(ii)证明 GL(2, **Q**)是 GL(2, **R**)的子群.

*H 2.55 举一个例子，使得群 G 的两个子群 H，K 的并集 $H\cup K$ 不是 G 的子群.

*2.56 设 G 是一个有限群，H，K 是它的两个子群. 证明，若 $H\leqslant K$，则

$$[G:H]=[G:K][K:H].$$

H 2.57 若 H，K 是群 G 的子群，且 $|H|$ 和 $|K|$ 互素，证明 $H\cap K=\{1\}$.

H 2.58 证明无限群有无限多个子群.

*2.59 设 G 是阶为 4 的群. 证明，要么 G 是循环群，要么对每个 $x\in G$ 有 $x^2=1$. 据此并利用习题 2.44 可知 G 一定是阿贝尔群.

2.60 (i)随机群 $\Sigma(2,\mathbf{R})$ 是由所有行和为 1 的非奇异 2×2 矩阵构成的. 证明，它是 $\mathrm{GL}(2,\mathbf{R})$ 的子群(见习题 2.48).

(ii)定义 $\Sigma'(2,\mathbf{R})$ 为所有非奇异**双随机矩阵**(所有行和为 1 且所有列和为 1)构成的集合. 证明，它是 $\mathrm{GL}(2,\mathbf{R})$ 的子群.

*H 2.61 设 G 是有限群，S 和 T 是非空子集(不必不相同). 证明，要么 $G=ST$，要么 $|G|\geqslant|S|+|T|$.

2.62 (i)若 $\{S_i: i\in I\}$ 是群 G 的一族子群，证明，陪集的交 $\bigcap_{i\in I}x_iS_i$ 或是空集或是 $\bigcap_{i\in I}S_i$ 的陪集.

H (ii)[**诺伊曼(B. H. Neumann)**]若群 G 是有限多个陪集的并，

$$G=x_1S_1\cup\cdots\cup x_nS_n,$$

158 证明至少有一个子群 S_i 在 G 中的指数是有限的.

2.63 (i)证明 S_3 中 $\langle(1\ 2)\rangle$ 的一个左陪集可以不等于 S_3 中 $\langle(1\ 2)\rangle$ 的一个右陪集，即存在 $\alpha\in S_3$ 使得 $\alpha\langle(1\ 2)\rangle\neq\langle(1\ 2)\rangle\alpha$.

H (ii)设 G 是一个有限群，且 $H\leqslant G$ 是子群. 证明 H 在 G 中的左陪集个数等于 H 在 G 中的右陪集个数.

→2.5 同态

有一个重要的问题需要解决，即两个给定的群 G 和 H 在某种意义上是否是相等的? 例如，我们知道，S_3 是 $X=\{1,2,3\}$ 的所有置换构成的群，S_Y 是 $Y=\{a,b,c\}$ 的所有置换构成的群. S_Y 不同于 S_3，这是因为 $\{1,2,3\}$ 的置换不同于 $\{a,b,c\}$ 的置换. 但是，虽然 S_3 和 S_Y 是不同的，但他们彼此之间的确存在极大的相似(见例 2.88). 正如我们将要看到的一样，同态和同构的概念允许我们比较不同的群.

→ **定义** 设 $(G,*)$ 和 $(H,\circ)$ 都是群(我们展示了它们中的运算)，则函数 $f:G\to H$ 是一个**同态**[⊖]，如果对所有 x，$y\in G$ 有

$$f(x*y)=f(x)\circ f(y).$$

若 f 还是双射，则称 f 为一个**同构**. 两个群 G 和 H 称为是**同构的**，记为 $G\cong H$，若它们之间存在一个同构 $f:G\to H$.

我们将在习题 2.67 中看到，同构是任意一族群上的等价关系. 特别地，若 $G\cong H$，则 $H\cong G$.

同态的两个明显的例子是恒等函数 $1_G:G\to G$ 和平凡同态 $f:G\to H$，对所有 $a\in G$ 有

⊖ "同态(homomorphism)"来自希腊词中意思是"相同的"的 homo 和意思是"形状"和"形式"的 morph. 因此一个同态把一个群带到另一个有类似形式的群(它的像)中. "同构(isomorphism)"含有意思是"相等的"的希腊词 iso，同构的群有完全相同的形式.

$f(a)=1$. 另外 1_G 还是一个同构.

还有一些更有趣的例子. 设$\mathbb{R}$是所有实数带上加法运算构成的群，并设$\mathbb{R}^>$是所有正实数带上乘法运算构成的群. 函数 $f:\mathbb{R}\to\mathbb{R}^>$, $f(x)=e^x$, 是一个同态，因为对任意 x, $y\in\mathbb{R}$ 有

$$f(x+y)=e^{x+y}=e^x e^y=f(x)f(y).$$ 159

f 还是一个同构，因为它存在反函数 $g:\mathbb{R}^>\to\mathbb{R}$, $x\mapsto\log(x)$. 因此，加法群$\mathbb{R}$与乘法群$\mathbb{R}^>$同构. 注意到反函数 g 也是一个同构:

$$g(xy)=\log(xy)=\log(x)+\log(y)=g(x)+g(y).$$

再看第二个例子，我们可以断言所有复数构成的加法群$\mathbb{C}$同构于加法群$\mathbb{R}^2$[见例 2.47(vi)]. 定义 $f:\mathbb{C}\to\mathbb{R}^2$ 为

$$f:a+ib\mapsto(a,b).$$

容易验证 f 是一个双射. f 是一个同态，因为

$$\begin{aligned}f([a+ib]+[a'+ib'])&=f([a+a']+i[b+b'])\\&=(a+a',b+b')\\&=(a,b)+(a',b')\\&=f(a+ib)+f(a'+ib').\end{aligned}$$

→ **定义** 设 G 是阶为 n 的有限群，a_1, a_2, …, a_n 是 G 的所有元素的一个无重复序列. G 的**乘法表**是指一个 $n\times n$ 矩阵，其 ij 元素是 a_ia_j.

G	a_1	…	a_j	…	a_n
a_1	a_1a_1	…	a_1a_j	…	a_1a_n
a_i	a_ia_1	…	a_ia_j	…	a_ia_n
a_n	a_na_1	…	a_na_j	…	a_na_n

让我们这样做：当写乘法表时，单位元列为第一个，即 $a_1=1$. 此时表的第一行和第一列是多余的，所以我们通常省略它们.

考虑两个几乎平凡的群：设 Γ_2 是乘法群$\{1, -1\}$，并设$\mathcal{P}$是奇偶群[例 2.47(vii)]. 以下是它们的乘法表：显然 Γ_2 和$\mathcal{P}$是不同的群，它们之间没有显著的区别也是显然的. 同构的概念使这一思想正规化. Γ_2 和$\mathcal{P}$是同构的，因为函数 $f:\Gamma_2\to\mathcal{P}$, $f(1)=$偶, $f(-1)=$奇，是一个同构，读者可以很快验证之.

Γ_2:

1	−1
−1	1

$\mathcal{P}$:

偶	奇
奇	偶

160

阶为 n 的群G有很多乘法表，这是因为它的元素有 $n!$ 种排法. 若 a_1, a_2, …, a_n 是G的所有元素的一个无重复序列，且 $f:G\to H$ 是一个双射，则 $f(a_1)$, $f(a_2)$, …, $f(a_n)$是 H 的所有元素的一个无重复序列，这样后一个序列确定了 H 的一个乘法表. f 是一个同构是说，若我们把 G 的乘法表[由 a_1, a_2, …, a_n 确定]添加到 H 的乘法表[由 $f(a_1)$, $f(a_2)$, …, $f(a_n)$确定]中，则两个乘法表相匹配：若 a_ia_j 是 G 的乘法表中的 ij 元素，则 $f(a_i)f(a_j)=$

$f(a_ia_j)$是 H 的乘法表中的 ij 元素. 在这个意义下，同构群有相同的乘法表. 因此同构群本质上是相同的，只是元素和运算的记号不同.

例 2.88 有一个可行的算法，可以检验群之间的双射 $f: G\to H$ 是否是同构的：列举 G 的元素a_1, …, a_n，写出由这个序列产生的 G 的乘法表，写出由序列 $f(a_1)$, …, $f(a_n)$产生的 H 的乘法表，然后逐行比较两个表中 n^2 个元素.

我们举例来阐述这种算法. $G=S_3$ 是$\{1, 2, 3\}$的所有置换构成的对称群，$H=S_Y$ 是 $Y=\{a, b, c\}$的所有置换构成的对称群. 首先，列举 G:

$$(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2).$$

我们定义一个明显的函数 $\varphi: S_3\to S_Y$，用字母代替数：

$$(1),(a\ b),(a\ c),(b\ c),(a\ b\ c),(a\ c\ b).$$

比较 S_3 的元素序列产生的乘法表和 S_Y 的元素序列产生的乘法表. 读者应当把每个 6×6 表都写出来，并把一个添加到另一个以看出它们是相配的. 我们将通过检验 4、5 位置上的元素来阐述这个事实. S_3 的乘法表中 4、5 位置上是积$(2\ 3)(1\ 2\ 3)=(1\ 3)$，而 S_Y 的乘法表中 4、5 位置上是积$(b\ c)(a\ b\ c)=(a\ c)$.

习题 2.65 推广了这个结论. ◀

我们回到更一般的同态上来.

引理 2.89 *设 $f: G\to H$ 是一个群同态，则*

(i) $f(1)=1$;

(ii) $f(x^{-1})=f(x)^{-1}$;

161 (iii) 对所有 $n\in\mathbb{Z}$ 有 $f(x^n)=f(x)^n$.

证明 (i)用 f 作用G 中等式 $1\cdot1=1$ 得到 H 中等式 $f(1)f(1)=f(1)$，两边乘以 $f(1)^{-1}$ 得 $f(1)=1$.

(ii)用 f 作用G 中等式 $x^{-1}x=1$ 得到 H 中等式 $f(x^{-1})f(x)=1$. 由命题 2.45(iv)逆元的唯一性知 $f(x^{-1})=f(x)^{-1}$.

(iii)用归纳法容易证明对所有 $n\geqslant0$ 有 $f(x^n)=f(x)^n$. 对于负指数，因为在一个群中 $(y^{-1})^n=y^{-n}$对所有 y 成立，所以

$$f(x^{-n})=f((x^{-1})^n)=f((x^{-1}))^n=(f(x)^{-1})^n=f(x)^{-n}.$$ ■

→ **例 2.90** 我们证明：若 G 和 H 都是阶为 m 的有限循环群，则 G 和 H 同构. 于是，由推论 2.87 知，任何两个阶为素数 p 的群同构.

假设 $G=\langle x\rangle$，$H=\langle y\rangle$. 定义 $f: G\to H$，$f(x^i)=y^i$，$0\leqslant i<m$. 现在 $G=\{1, x, x^2, \cdots, x^{m-1}\}$，$H=\{1, y, y^2, \cdots, y^{m-1}\}$，所以 f 是双射. 为看出 f 是一个同态(因而是一个同构)，我们必须证明对所有 i，j，$0\leqslant i$，$j<m$，有 $f(x^ix^j)=f(x^i)f(x^j)$. 若 $i+j<m$，这个等式显然成立，因为 $f(x^{i+j})=y^{i+j}$,

$$f(x^ix^j)=f(x^{i+j})=y^{i+j}=y^iy^j=f(x^i)f(x^j).$$

若 $i+j\geqslant m$，则 $i+j=m+r$，其中 $0\leqslant r<m$，所以

$$x^{i+j}=x^{m+r}=x^mx^r=x^r$$

(因为 $x^m=1$). 类似地, $y^{i+j}=y^r$(因为 $y^m=1$). 因而

$$f(x^ix^j) = f(x^{i+j}) = f(x^r) = y^r = y^{i+j} = y^iy^j = f(x^i)f(x^j).$$

因此, f 是一个同构, 且 $G\cong H$. (例 2.117 将给出一个更好的证明.) ◀

群 G 与跟它同构的群所共有的性质称为群 G 的**不变量**. 例如, 阶 $|G|$ 是群 G 的不变量, 因为同构的群有相同的阶. 交换律是不变量[若 a 和 b 交换, 则 $ab=ba$ 且

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a),$$

因而, $f(a)$和 $f(b)$交换]. 因此, $\mathbb{R}$ 和 $GL(2, \mathbb{R})$不同构, 因为$\mathbb{R}$ 是阿贝尔群而 $GL(2, \mathbb{R})$不是. 群还有其他的不变量(见习题 2.69). 一般地, 判断两个给定的群是否同构是一个有挑战性的问题. 162

→ **例 2.91** 下面我们给出阶相同但不同构的两个群.

和在例 2.67(ii)中一样, 设 $\mathbf{V}$ 是由下列四个置换构成的四元群:

$$\mathbf{V} = \{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\},$$

并设 $\Gamma_4=\langle i\rangle=\{1, i, -1, -i\}$是由四次单位根构成的乘法循环群, 其中 $i^2=-1$. 假设存在同构 $f: \mathbf{V}\to\Gamma_4$, 则由 f 是满射知存在 $x\in\mathbf{V}$ 使得 $i=f(x)$. 但对所有 $x\in\mathbf{V}$ 有 $x^2=(1)$, 所以 $i^2=f(x)^2=f(x^2)=f((1))=1$, 此与 $i^2=-1$ 矛盾. 因此, $\mathbf{V}$ 和 Γ_4 不同构.

这个结论还有其他的证法. 例如, Γ_4 是循环群而 $\mathbf{V}$ 不是, 或者 Γ_4 有一个阶为 4 的元素而 $\mathbf{V}$ 没有, 或者 Γ_4 只有一个阶为 2 的元素而 $\mathbf{V}$ 有 3 个阶为 2 的元素. 到这时, 你应该真的相信 Γ_4 和 $\mathbf{V}$ 不同构吧! ◀

→ **定义** 设 $f: G\to H$ 是一个同态, 定义 f 的**核**[⊖]

$$\mathbf{kernel}f = \{x \in G: f(x) = 1\}$$

和 f 的**象**

$$\mathbf{image}f = \{h \in H: \text{存在 } x \in G \text{ 使 } h = f(x)\}.$$

我们通常将 kernel$f$, image$f$ 分别缩写为 ker$f$, im$f$.

例 2.92 (i)若 $\Gamma_n=\langle\zeta\rangle$, 其中 $\zeta=e^{2\pi i/n}$是 n 次本原单位根, 则 $f: \mathbb{Z}\to\Gamma_n$, $f(m)=\zeta^m$, 是一个满同态, 其核 ker$f$ 是 n 的所有倍数.

(ii)若 Γ_2 是乘法群 $\Gamma_2=\{\pm1\}$, 则定理 2.39 是说 sgn: $S_n\to\Gamma_2$ 是一个同态. sgn 的象是 $\{\pm1\}$, 即 sgn 是满射, 因为对于对换 τ 有 sgn$(\tau)=-1$. sgn 的核是由所有偶置换构成的交错群 A_n.

(iii)行列式 det: $GL(2, \mathbb{R})\to\mathbb{R}^\times$是一个同态, 这里$\mathbb{R}^\times$是所有非零实数构成的乘法群. 当 $r\in\mathbb{R}^\times$ 时 $r=\det\left(\begin{bmatrix} r & 0 \\ 0 & 1\end{bmatrix}\right)$, 所以 im det$=\mathbb{R}^\times$, 即 det 是满射. det 的核是特殊线性群 $SL(2, \mathbb{R})$. [这个例子可以推广到 $GL(n, \mathbb{R})$, 见例 2.48(ii).] 163

(iv)设 $f: G\to H$ 是一个同态, ker$f=K$. 回忆函数逆象的定义: 若 $f: X\to Y$ 是函数, $B\subseteq Y$, 则

⊖ "核(kernel)"来自意思是"谷粒"或"种子"的德语词. 在这里它指出了同态的一个重要成分.

$$f^{-1}(B)=\{x\in X: f(x)\in B\}.$$

若 $f: G\to H$ 是一个同态，且 $B\leqslant H$ 是 H 的子群，则我们证明 $f^{-1}(B)$ 是 G 的子群. 现在 $1\in f^{-1}(B)$，因为 $f(1)=1\in B\leqslant H$. 若 x，$y\in f^{-1}(B)$，则 $f(x)$，$f(y)\in B$，所以 $f(x)f(y)\in B$，因而 $f(xy)=f(x)f(y)\in B$，$xy\in f^{-1}(B)$. 最后，若 $x\in f^{-1}(B)$，则 $f(x)\in B$，因而 $f(x^{-1})=f(x)^{-1}\in B$，$x^{-1}\in f^{-1}(B)$. 特别地，若 $B=\{1\}$，则 $f^{-1}(B)=f^{-1}(1)=\ker f$. 于是，若 $f: G\to H$ 是一个同态，B 是 H 的子群，则 $f^{-1}(B)$ 是 G 的包含 $\ker f$ 的子群. ◀

命题 2.93 设 $f: G\to H$ 是一个同态，则

(i) $\ker f$ 是 G 的子群，$\operatorname{im} f$ 是 H 的子群.

(ii) 若 $x\in\ker f$ 且 $a\in G$，则 $axa^{-1}\in\ker f$.

(iii) f 是单射当且仅当 $\ker f=\{1\}$.

证明 (i) 由引理 2.89 知 $1\in\ker f$，因为 $f(1)=1$. 其次，若 x，$y\in\ker f$，则 $f(x)=1=f(y)$，因此 $f(xy)=f(x)f(y)=1\cdot 1=1$，所以 $xy\in\ker f$. 最后，若 $x\in\ker f$，则 $f(x)=1$，所以 $f(x^{-1})=f(x)^{-1}=1^{-1}=1$，因此 $x^{-1}\in\ker f$，$\ker f$ 是 G 的子群.

现在证明 $\operatorname{im} f$ 是 H 的子群. 首先，$1=f(1)\in\operatorname{im} f$. 其次，若 $h=f(x)\in\operatorname{im} f$，则 $h^{-1}=f(x)^{-1}=f(x^{-1})\in\operatorname{im} f$. 最后，若 $k=f(y)\in\operatorname{im} f$，则 $hk=f(x)f(y)=f(xy)\in\operatorname{im} f$. 因此 $\operatorname{im} f$ 是 H 的一个子群.

(ii) 若 $x\in\ker f$，则 $f(x)=1$ 且

$$f(axa^{-1})=f(a)f(x)f(a)^{-1}=f(a)1f(a)^{-1}=f(a)f(a)^{-1}=1,$$

因此 $axa^{-1}\in\ker f$.

(iii) 若 f 是单射，则 $x\neq 1$ 可推出 $f(x)\neq f(1)=1$，所以 $x\notin\ker f$. 反之，假设 $\ker f=\{1\}$，且 $f(x)=f(y)$，则 $1=f(x)f(y)^{-1}=f(xy^{-1})$，所以 $xy^{-1}\in\ker f=1$，因此 $xy^{-1}=1$，$x=y$，f 是单射. ■

定义 群 G 的子群 K 称为 G 的**正规子群**，如果当 $k\in K$ 和 $g\in G$ 时有 $gkg^{-1}\in K$. 若 K 是群 G 的一个正规子群，则记为

164 $$K\lhd G.$$

命题 2.93 是说，同态的核总是正规子群. 若 G 是一个阿贝尔群，则它的任何子群 K 都是正规的，这是因为若 $k\in K$，$g\in G$，则 $gkg^{-1}=kgg^{-1}=k\in K$.

S_3 的循环子群 $H=\langle(1\ 2)\rangle=\{(1),(1\ 2)\}$ 不是 S_3 的正规子群：若 $\alpha=(1\ 2\ 3)$，则 $\alpha^{-1}=(3\ 2\ 1)$，且

$$\alpha(1\ 2)\alpha^{-1}=(1\ 2\ 3)(1\ 2)(3\ 2\ 1)=(2\ 3)\notin H.$$

另一方面，S_3 的循环子群 $K=\langle(1\ 2\ 3)\rangle$ 是正规子群，读者可以自己验证.

由例 2.92(ii) 和 (iii) 知 A_n 是 S_n 的正规子群，$\mathrm{SL}(2,\mathbb{R})$ 是 $\mathrm{GL}(2,\mathbb{R})$ 的正规子群（这些结论很容易证明）.

定义 设 G 是一个群且 $a\in G$，则 G 中形如

$$gag^{-1}$$

的元素称为 a 的**共轭**，其中 $g\in G$.

显然，子群 $K \leqslant G$ 是正规子群当且仅当 K 包含其元素的所有共轭：若 $k \in K$，则对所有 $g \in G$ 有 $gkg^{-1} \in K$. 在命题 2.33 中，我们证明了 α，$\beta \in S_n$ 在 S_n 中共轭当且仅当它们有相同的循环结构.

若 $H \leqslant S_n$，则 α，$\beta \in H$ 在 S_n 中共轭(即 α 和 β 有相同的循环结构)不能推出 α 和 β 在 H 中共轭. 例如，(1 2)(3 4)和(1 3)(2 4)在 S_4 中共轭，这是因为它们有相同的循环结构，但是它们在 **V** 中不共轭，因为四元群 **V** 是阿贝尔群.

注 在线性代数中，如果我们利用 V 的一个基，则线性变换 $T: V \to V$ 决定一个 $n \times n$ 矩阵 A，其中 V 是 $\mathbb{R}$ 上的 n 维向量空间. 如果利用另一个基，则可以由 T 得到另一个矩阵 B. 可以证明 A 和 B 相似，即存在非奇异矩阵 P 满足 $B = PAP^{-1}$. 因此，在 $\mathrm{GL}(n, \mathbb{R})$ 中共轭元是相似的.

→ **定义** 设 G 是群且 $g \in G$，对所有 $a \in G$，定义**共轭映射** $\gamma_g: G \to G$ 为

$$\gamma_g(a) = gag^{-1}$$ 165

命题 2.94 (i)设 G 是群且 $g \in G$，则共轭映射 $\gamma_g: G \to G$ 是一个同构.

(ii)共轭元素有相同的阶.

证明 (i)若 g，$h \in G$，则

$$(\gamma_g \circ \gamma_h)(a) = \gamma_g(hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = \gamma_g h(a);$$

即，

$$\gamma_g \circ \gamma_h = \gamma_{gh}.$$

于是每个 γ_g 是一个双射，这是因为 $\gamma_g \circ \gamma_{g^{-1}} = \gamma_1 = 1 = \gamma_{g^{-1}} \circ \gamma_g$. 我们现在证明 γ_g 是一个同构：若 a，$b \in G$，则

$$\gamma_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \gamma_g(a)\gamma_g(b).$$

(ii)设 a，b 是共轭的，也就是说存在 $g \in G$ 使得 $b = gag^{-1}$，即 $b = \gamma_g(a)$. 因为 γ_g 是一个同构，所以由习题 2.69(ii)知 a 和 $b = \gamma_g(a)$ 有相同的阶. ∎

→ **例 2.95** 定义群 G 的**中心** $Z(G)$ 如下：

$$Z(G) = \{z \in G: \text{对所有 } g \in G \text{ 有 } zg = gz\},$$

即，$Z(G)$是由 G 中所有能和任意元素交换的元素构成的. (注意等式 $zg = gz$ 可以写为 $z = gzg^{-1}$，因此 G 中没有其他元素和 z 是共轭的.)

我们证明 $Z(G)$是 G 的子群. 显然，$1 \in Z(G)$，因为 1 与任意元素交换. 若 y，$z \in Z(G)$，则对所有 $g \in G$ 有 $yg = gy$，$zg = gz$. 因此，$(yz)g = y(zg) = y(gz) = (yg)z = g(yz)$，所以 yz 与任意元素交换，$yz \in Z(G)$. 最后，若 $z \in Z(G)$，则对所有 $g \in G$ 有 $zg = gz$. 特别地，$zg^{-1} = g^{-1}z$. 因此，

$$gz^{-1} = (zg^{-1})^{-1} = (g^{-1}z)^{-1} = z^{-1}g$$

[我们利用了引理 2.46：$(ab)^{-1} = b^{-1}a^{-1}$ 和 $(a^{-1})^{-1} = a$].

中心 $Z(G)$是正规子群：若 $z \in Z(G)$且 $g \in G$，则

$$gzg^{-1} = zgg^{-1} = z \in Z(G).$$

群 G 是阿贝尔群当且仅当 $Z(G)=G$. 相反地，若 $Z(G)=\{1\}$，则称群 G **无中心**. 例如，易知 $Z(S_3)=\{1\}$. 事实上，所有大的对称群都是无中心的，因为由习题 2.34 知对所有 $n\geq 3$ 有
166 $Z(S_n)=\{1\}$. ◀

→ **例 2.96** 四元群 $\mathbf{V}$ 是 S_4 的正规子群. 回忆 $\mathbf{V}$ 的元素是

$$\mathbf{V}=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}.$$

根据命题 2.32，两个对换的积的每个共轭元是另一个这样的元素. 但是在例 2.29 中，我们看到 S_4 中只有 3 个置换有这样的循环结构，所以 $\mathbf{V}$ 是 S_4 的正规子群. ◀

→ **命题 2.97** (i)若 H 是群 G 中指数为 2 的子群，则对任意 $g\in G$ 有 $g^2\in H$.

(ii)若 H 是群 G 中指数为 2 的子群，则 H 是 G 的正规子群.

证明 (i)因为 H 的指数为 2，所以仅存在两个陪集 H 和 aH，其中 $a\notin H$. 因此，G 是无交并 $G=H\cup aH$，即 aH 是 H 的补集. 取 $g\in G$ 但 $g\notin H$，使得 $g\in aH$，即存在 $h\in H$ 使得 $g=ah$. 类似地，若 $g^2\notin H$，则 $g^2=ah'$，其中 $h'\in H$. 因此

$$g=g^{-1}g^2=(ah)^{-1}ah'=h^{-1}a^{-1}ah'=h^{-1}h'\in H,$$

矛盾.

(ii)只须证明：若 $h\in H$，则对任意 $g\in G$，共轭元素 $ghg^{-1}\in H$. 正如在(i)中所提到的，H 的指数为 2 是说 aH 是 H 的补集. 现在，要么 $g\in H$ 要么 $g\in aH$. 若 $g\in H$，则 $ghg^{-1}\in H$，因为 H 是一个子群. 若 $g\in aH$，则记 $g=ax$，其中 $x\in H$. 则 $ghg^{-1}=a(xhx^{-1})a^{-1}=ah'a^{-1}$，其中 $h'=xhx^{-1}\in H$(因为 h'是 H 中三个元素的乘积). 假设 $ghg^{-1}\notin H$，则 $ghg^{-1}=ah'a^{-1}\in aH$，即存在 $y\in H$ 使 $ah'a^{-1}=ay$. 消去 a 得 $h'a^{-1}=y$，则 $a=y^{-1}h'\in H$，矛盾. 因此，若 $h\in H$ 则 h 的每个共轭元都在 H 中. 即 H 是 G 的正规子群. ■

→ **定义** 由 $GL(2,\mathbb{C})$中的矩阵构成的阶为 8 的群

$$\mathbf{Q}=\{I,A,A^2,A^3,B,BA,BA^2,BA^3\}$$

167 称为**四元数群**[⊖]，其中 I 是单位矩阵，$A=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$，$B=\begin{bmatrix}0&i\\i&0\end{bmatrix}$.

读者应该注意 $A\in\mathbf{Q}$ 的阶为 4，因此$\langle A\rangle$是阶为 4 的子群，因而指数为 2，另一个陪集是 $B\langle A\rangle=\{B, BA, BA^2, BA^3\}$.

例 2.98 在习题 2.86 中，读者可以验证 $\mathbf{Q}$ 是阶为 8 的非阿贝尔群. 我们断言 $\mathbf{Q}$ 的每个子群都是正规子群. 拉格朗日定理是说 $\mathbf{Q}$ 的每个子群的阶是 8 的因子，所以子群的阶只可能是 1、2、4 和 8. 显然，子群{1}以及阶为 8 的子群(即 $\mathbf{Q}$ 本身)都是正规子群. 由命题 2.97(ii)知

⊖ 加、减、乘、除(除数不为 0)这四个运算可以从$\mathbb{R}$推广到平面上，使得算术的所有普通法则都成立. 当然，在这个背景下，平面通常称为复数集$\mathbb{C}$. 哈密尔顿(W. R. Hamilton)发明了一种方法，将这些运算从$\mathbb{C}$推广到四维空间，使得算术的所有普通法则都成立(除了乘法交换律). 他称这些新"数"为"四元数(quaternions)"(来自拉丁文中意思是"四"的词). 通过给出四个特殊的四元组 1，i，j，k 的积来确定乘法.

$$\mathbf{i}^2=-1=\mathbf{j}^2=\mathbf{k}^2;$$

$$\mathbf{ij}=\mathbf{k};\quad \mathbf{ji}=-\mathbf{k};\quad \mathbf{jk}=\mathbf{i};\quad \mathbf{kj}=-\mathbf{i};\quad \mathbf{ki}=\mathbf{j};\quad \mathbf{jk}=-\mathbf{j}.$$

所有非零四元数构成一个乘法群，且四元数群是包含这四个元素的最小子群(阶为 8).

阶为 4 的子群一定是正规的，因为它的指数为 2. 最后，**Q** 中阶为 2 的元素只有 $-I$，读者可以很快验证之，所以 $\langle -I\rangle$ 是阶为 2 的唯一子群. 但是这个子群是正规子群，因为若 M 是任意一个矩阵，则 $M(-I)=(-I)M$，所以 $M(-I)M^{-1}=(-I)MM^{-1}=-I\in\langle -I\rangle$. [习题 2.86 要求我们证明 $\langle -I\rangle=Z(\mathbf{Q})$.] ◀

例 2.98 表明，**Q** 是非阿贝尔群，因为每个子群是正规的，所以它类似阿贝尔群. 实质上这样的例子只有一个：其子群都为正规子群的有限群具有 $\mathbf{Q}\times A$ 的形式，其中 A 有特殊形式：$A=B\times C$ 的阿贝尔群，其中 B 的每个非单位元元素的阶为 2，C 的每个元素的阶是奇数(直积 $A\times B$ 将在下一节介绍).

拉格朗日定理是说有限群 G 的子群的阶一定是 $|G|$ 的因子. 这隐含着一个问题：给定 $|G|$ 的某个因子 d，G 是否一定有阶为 d 的子群？下面这个结论告诉我们：不一定存在这样的子群.

→ **命题 2.99** 交错群 A_4 的阶为 12，但它没有阶为 6 的子群.

证明 首先，由习题 2.32 知 $|A_4|=12$. 假设 A_4 有一个阶为 6 的子群 H，则 H 的指数为 2，由推论 2.97(i)知，对任意 $\alpha\in A_4$ 有 $\alpha^2\in H$. 但是，若 α 是一个 3-循环置换，则 α 的阶为 3，所以 $\alpha=\alpha^4=(\alpha^2)^2$. 因此，$H$ 包含每个 3-循环置换. 此与 A_4 中有 8 个 3-循环置换相矛盾. ■ 168

命题 2.124 将证明：若 G 是阶为 n 的阿贝尔群，则对 n 的每个因子 d，G 确实有阶为 d 的子群.

习题

H 2.64 判断对错并说明理由.

(i)若 G，H 都是加法群，则每个同态 $f: G\to H$ 满足：对所有 x，$y\in G$ 有 $f(x+y)=f(x)+f(y)$.

(ii)函数 f: $\mathbf{R}\to\mathbf{R}^\times$ 是同态当且仅当对所有 x，$y\in\mathbf{R}$ 有 $f(x+y)=f(x)+f(y)$.

(iii)包含 $\mathbf{Z}\to\mathbf{R}$ 是加法群同态.

(iv)$\mathbf{Z}$ 的子群 $\{0\}$ 与 S_5 的子群 $\{(1)\}$ 同构.

(v)阶相同的任意两个有限群同构.

(vi)若 p 是素数，则阶为 p 的任意两个群同构.

(vii)子群 $\langle(1\ 2)\rangle$ 是 S_3 的正规子群.

(viii)子群 $\langle(1\ 2\ 3)\rangle$ 是 S_3 的正规子群.

(ix)若 G 是群，则 $Z(G)=G$ 当且仅当 G 是阿贝尔群.

(x)3-循环置换 $(7\ 6\ 5)$ 和 $(5\ 26\ 34)$ 在 S_{100} 中共轭.

*H 2.65 若存在双射 $f: X\to Y$(即，若 X 和 Y 有相同的元素个数)，证明存在同构 $\varphi: S_X\to S_Y$.

2.66 设 G 是群，X 是集合，$\varphi: G\to X$ 是双射. 证明，X 上存在一个运算使 X 作成群，且使得 $\varphi: G\to X$ 是一个同构.

*2.67 (i)证明，同态的合成是同态.

(ii)证明，同构的逆是同构.

(iii)证明，在任意一族群上同构是一个等价关系.

(iv)证明，若两个群都与第三个群同构，则这两个群同构.

2.68 证明，群 G 是阿贝尔群当且仅当函数 $f: G\to G$，$f(a)=a^{-1}$ 是一个同态.

*2.69 这个习题给出了群 G 的一些不变量. 设 $f: G \to H$ 是一个同构.

(i)证明，若 $a \in G$ 有无限阶，则 $f(a)$ 有无限阶，若 a 的阶为 n，则 $f(a)$ 的阶为 n. 由此得出，若 G 有一个元素的阶为 n，而 H 没有阶为 n 的元素，则 $G \not\cong H$.

(ii)证明，若 $G \cong H$，则对 $|G|$ 的每个因子 k，G 和 H 有相同个数的阶为 k 的元素.

2.70 (i)证明，每个满足 $|G|<6$ 的群 G 是阿贝尔群.

(ii)求出两个阶为 6 的非同构群.

2.71 证明，阶为 4 的二面体群与 4 元群 $\mathbf{V}$ 同构，阶为 6 的二面体群与 S_3 同构.

169 *2.72 证明，阶为 $2n$ 的任意两个二面体群同构.

*2.73 这个习题是给熟悉 $n \times n$ 矩阵(看例 4.66)的读者做的. 定义函数 $f: S_n \to \mathrm{GL}(n, \mathbb{R})$，$f: \sigma \mapsto P_\sigma$，其中 P_σ 是一个矩阵(称为置换矩阵)，是用 σ 置换 $n \times n$ 单位矩阵 I 的列而得到的矩阵. 证明 f 是 S_n 与 $\mathrm{GL}(n, \mathbb{R})$ 的一个子群之间的同构.

2.74 (i)求一个子群 $H \leqslant S_4$，满足 $H \cong \mathbf{V}$ 但 $H \neq \mathbf{V}$.

(ii)证明(i)中的子群 H 不是正规子群.

H 2.75 设 G 是群且 $a, b \in G$，证明，ab 和 ba 有相同的阶.

2.76 (i)若 $f: G \to H$ 是一个同态且 $x \in G$ 的阶为 k，证明，$f(x) \in H$ 的阶为 m，其中 $m \mid k$.

(ii)若 $f: G \to H$ 是一个同态且 $(|G|, |H|)=1$，证明，对所有 $x \in G$ 有 $f(x)=1$.

*2.77 H (i)证明特殊正交群 $SO(2, \mathbb{R})$ 与循环群 S^1 同构.

(ii)证明，平面上绕原点的所有旋转在合成运算下作成一个群，且与 $SO(2, \mathbb{R})$ 同构.

H 2.78 设 G 是系数在 $\mathbb{Z}$ 中的关于 x 的所有多项式构成的加法群，H 是所有正有理数构成的乘法群. 证明 $G \cong H$.

*2.79 证明，若 H 是一个子群，满足对每个 $b \in G$ 有 $bH = Hb = \{hb: h \in H\}$，则 H 是正规子群. (其逆命题已在引理 2.112 中证明.)

2.80 证明，群 G 的任意一族正规子群的交还是 G 的正规子群.

2.81 定义 $W = \langle (1\ 2)(3\ 4) \rangle$，即 S_4 的由 $(1\ 2)(3\ 4)$ 生成的循环子群. 证明 W 是 $\mathbf{V}$ 的正规子群，但是 W 不是 S_4 的正规子群. 由此得出正规性不能传递：$K \lhd H$ 和 $H \lhd G$ 不一定能推出 $K \lhd G$.

*H 2.82 设 G 是有限乘法群. 证明，若 $|G|$ 是奇数，则每个 $x \in G$ 有唯一的平方根. 利用习题 2.45 得出恰存在一个 $g \in G$ 使得 $g^2 = x$.

H 2.83 给出一个群 G，一个子群 $H \leqslant G$ 和一个元素 $g \in G$，使得 $[G:H]=3$ 和 $g^3 \notin H$.

*H 2.84 证明，$\mathrm{GL}(2, \mathbb{R})$ 的中心是所有纯量矩阵 $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ 构成的集合，其中 $a \neq 0$.

*2.85 设 $\zeta = e^{2\pi i/n}$ 是一个 n 次本原单位根，定义 $A = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix}$，$B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

(i)证明，A 的阶为 n，B 的阶为 2.

(ii)证明，$BAB = A^{-1}$.

H (iii)证明，形如 A^i 和 BA^i 的矩阵构成乘法子群 $G \leqslant \mathrm{GL}(2, \mathbb{C})$，其中 $0 \leqslant i < n$.

(iv)证明，G 中每个矩阵有形如 $B^i A^j$ 的唯一表达式，其中 $i=0, 1$，$0 \leqslant j < n$. 由此得 $|G| = 2n$ 和 $G \cong D_{2n}$.

*2.86 回忆四元数群 $\mathbf{Q}$(定义见例 2.98)是由 $\mathrm{GL}(2, \mathbb{C})$ 中的 8 个矩阵构成的，

$$\mathbf{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\},$$

其中 $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$，$B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

H (i)证明，Q在矩阵乘法运算下是非阿贝尔群.

(ii)证明，$-I$是Q中阶为2的唯一元素，而所有其他元素$M\neq I$满足$M^2=-I$. [170]

(iii)证明，Q有阶为2的唯一子群且它是Q的中心.

(iv)证明，$\langle -I\rangle$是中心$Z(\mathbf{Q})$.

*H 2.87 证明，四元数群Q和二面体群D_8的阶都为8且不同构.

2.88 设G是由两个阶为2的元素生成的有限群，证明存在某个$n\geqslant 2$使得$G\cong D_{2n}$.

*2.89 (i)证明，A_3是S_3的阶为3的唯一子群.

H (ii)证明，A_4是S_4的阶为12的唯一子群.（在习题2.135中，这个结论可从S_4和A_4推广到对S_n和A_n成立，$n\geqslant 3$.）

*2.90 (i)设$\mathcal{A}$是由所有形如$A=\begin{bmatrix} a & b \\ 0 & 1\end{bmatrix}$的$2\times 2$矩阵构成的集合，其中$a\neq 0$. 证明$\mathcal{A}$是$\mathrm{GL}(2,\mathbb{R})$的子群.

(ii)证明ψ: $\mathrm{Aff}(1,\mathbb{R})\to\mathcal{A}$，$f\mapsto A$，是一个同构，其中$f(x)=ax+b$[见例2.48(iv)].

H (iii)通过证明φ: $\Sigma(2,\mathbb{R})\to\mathcal{A}\cong\mathrm{Aff}(1,\mathbb{R})$，$\varphi(M)=QMQ^{-1}$，是一个同构，其中$Q=\begin{bmatrix} 1 & 0 \\ 1 & 1\end{bmatrix}$，$Q^{-1}=\begin{bmatrix} 1 & 0 \\ -1 & 1\end{bmatrix}$，来证明随机群$\Sigma(2,\mathbb{R})$[见习题2.48]与仿射群$\mathrm{Aff}(1,\mathbb{R})$同构.

H 2.91 证明，对称群$\Sigma(\pi_n)$与S_n的一个子群同构，其中π_n是正n边形.

2.92 群G的一个自同构是指同构$G\to G$.

(i)证明，群G的所有自同构构成的集合$\mathrm{Aut}(G)$在合成运算下作成群.

(ii)证明，$\gamma: G\to\mathrm{Aut}(G)$，$g\mapsto\gamma_g$是一个同态.

(iii)证明，$\ker\gamma=Z(G)$.

(iv)证明，$\mathrm{im}\gamma\lhd\mathrm{Aut}(G)$.

2.93 设G是群，证明，$\mathrm{Aut}(G)=\{1\}$当且仅当$|G|\leqslant 2$.

2.94 设C是阶为n的有限循环群，证明，$|\mathrm{Aut}(C)|=\phi(n)$，其中$\phi(n)$是欧拉$\phi$-函数.

→2.6 商群

我们将利用模m同余来构造群. 一旦做到了，我们将能够利用群的理论证明费马定理. 这种构造的原型是用给定的群去建立一个新群(叫做商群).

回忆一下，给定$m\geqslant 2$和$a\in\mathbb{Z}$，则a模m的同余类是$\mathbb{Z}$的子集$[a]$：

$$\begin{aligned}[a] &= \{b\in\mathbb{Z}: b\equiv a \bmod m\} \\ &= \{a+km: k\in\mathbb{Z}\} \\ &= \{\cdots,a-2m,a-m,a,a+m,a+2m,\cdots\}.\end{aligned}$$ [171]

→ **定义** 所有模m的同余类构成的族称为**模m整数类**，记为$\mathbb{I}_m$[⊖].

例如，若$m=2$，则$[0]=\{b\in\mathbb{Z}: b\equiv 0 \bmod 2\}$是所有偶数构成的集合，$[1]=\{b\in\mathbb{Z}: b\equiv$

⊖ 今天，用$\mathbb{Z}$表示所有整数构成的集合被广泛地接受，且模m整数类的两个很流行的记号是$\mathbb{Z}/m\mathbb{Z}$和$\mathbb{Z}_m$. 两个记号都有优点：第一个记号使人想起该群是$\mathbb{Z}$的商群，但是该记号有点笨重；第二个记号很紧凑，但是会引起麻烦，因为当m是素数p时，它被数论学家们用来表示所有分母与p互素的有理数(p进分数环). 实际上，许多数论学家用$\mathbb{Z}_p$表示p进整数环. 为避免可能出现的麻烦，我们引入记号$\mathbb{I}_m$.

1 mod 2}是所有奇数构成的集合. 注意到$[2]=\{2+2k: k\in\mathbb{Z}\}$也是所有偶数构成的集合，所以$[0]=[2]$. 事实上，$[0]=[2]=[-2]=[4]=[-4]=[6]=[-6]=\cdots$.

注 给定m，我们可以得到$\mathbb{Z}$的由m生成的循环子群$\langle m\rangle$. 在例2.18(ii)中，我们看到同余类$[a]$正是陪集$a+\langle m\rangle$.

记号$[a]$是不完善的，因为它没有提到模m：例如，$\mathbb{I}_2$中的$[1]$不同于$\mathbb{I}_3$中的$[1]$(前者是所有奇数构成的集合，后者是$\{1+3k: k\in\mathbb{Z}\}=\{\cdots, -2, 1, 4, 7, \cdots\}$). 这不会引起麻烦，因为我们通常一次只处理一个$\mathbb{I}_m$. 如果存在引起麻烦的危险，如在定理2.128中，我们将用$[a]_m$表示$\mathbb{I}_m$中a的同余类. 下面这个命题是引理2.19关于等价类的特殊情形.

→ **命题 2.100** 在$\mathbb{I}_m$中，$[a]=[b]$当且仅当$a\equiv b \bmod m$.

证明 若$[a]=[b]$，则$a\in[a]$，由传递性知，$a\in[a]=[b]$，因此$a\equiv b \bmod m$.

反之，若$c\in[a]$，则$c\equiv a \bmod m$，所以由传递性知$c\equiv b \bmod m$. 因而$[a]\subseteq[b]$. 根据对称性，$b\equiv a \bmod m$，由此得$[b]\subseteq[a]$. 因此$[a]=[b]$. ■

总之，命题2.100是说，若用同余类代替数，则数之间的模m同余可以转化为相等.

特别地，在$\mathbb{I}_m$中$[a]=[0]$当且仅当$a\equiv 0 \bmod m$，即$[a]=[0]$当且仅当m是a的因子.

命题 2.101 给定$m\geqslant 2$.

172 (i)若$a\in\mathbb{Z}$，则存在r使得$[a]=[r]$，$0\leqslant r<m$.

(ii)若$0\leqslant r'<r<m$，则$[r']\neq[r]$.

(iii)$\mathbb{I}_m$恰有m个元素，即$[0]$，$[1]$，…，$[m-1]$.

证明 (i)对每个$a\in\mathbb{Z}$，除法算式给出$a=qm+r$，其中$0\leqslant r<m$，因而$a-r=qm$，$a\equiv r \bmod m$. 因此$[a]=[r]$，其中r是a被m除后的余数.

(ii)由命题1.58(ii)知$r'\not\equiv r \bmod m$.

(iii)由(i)知$\mathbb{I}_m$中每个元素$[a]$取自序列$[0]$，$[1]$，$[2]$，…，$[m-1]$. 由(ii)知这m个元素没有重复. ■

我们将让$\mathbb{I}_m$带上加法运算使之成为一个阿贝尔群. 命题2.100是说，$\mathbb{I}_m$中$[a]=[b]$当且仅当$a\equiv b \bmod m$，所以$[a]\in\mathbb{I}_m$有许多名称. 我们给$\mathbb{I}_m$定义的运算将依赖于名称的选择，所以我们不得不证明这个运算是定义良好的.

引理 2.102 若$m\geqslant 2$，则函数$\alpha: \mathbb{I}_m\times\mathbb{I}_m\to\mathbb{I}_m$，

$$\alpha([a],[b])=[a+b],$$

是$\mathbb{I}_m$上的一个运算.

证明 为看出α是(定义良好的)函数，我们必须证明，若$[a]=[a']$和$[b]=[b']$，则$\alpha([a],[b])=\alpha([a'],[b'])$，即$[a+b]=[a'+b']$. 但这正是命题1.60(i). ■

→ **命题 2.103** 若$m\geqslant 2$，则$\mathbb{I}_m$是加法循环群，其阶为m，生成元为$[1]$.

证明 仅在这个证明中，我们用田表示同余类的加法运算：

$$\alpha([a],[b])=[a]\boxplus[b]=[a+b].$$

由普通加法满足结合律得运算田满足结合律：

$$[a]\boxplus([b]\boxplus[c])=[a]\boxplus[b+c]$$

$$
\begin{aligned}
&=[a+(b+c)]\\
&=[(a+b)+c]\\
&=[a+b]\boxplus[c]\\
&=([a]\boxplus[b])\boxplus[c].
\end{aligned}
$$

由普通加法满足交换律得运算田满足交换律：

$$[a]\boxplus[b]=[a+b]=[b+a]=[b]\boxplus[a].$$ 173

单位元是[0]：因为 0 是Z 的加法单位元，所以

$$[0]\boxplus[a]=[0+a]=[a].$$

$[a]$的逆元是$[-a]$：因为$-a$ 是 a 在Z 中的加法逆元，所以

$$[-a]\boxplus[a]=[-a+a]=[0].$$

因此，$\mathbb{I}_m$ 是阶为 m 的阿贝尔群. 它是由[1]生成的循环群，这是因为若 $0\leqslant r<m$，则 $[r]=[1]+\cdots+[1]$等于 r 个[1]相加. ■

读者应当注意到$\mathbb{I}_m$ 的群公理是从Z 的群公理中“遗传”过来的.

以下是群$\mathbb{I}_m$ 的另一种构造. 定义 G_m 为集合$\{0,1,\cdots,m-1\}$，并在 G_m 上定义一个运算为

$$a\boxplus b=\begin{cases}a+b & \text{若 } a+b\leqslant m-1;\\ a+b-m & \text{若 } a+b>m-1.\end{cases}$$

尽管这个定义比我们刚才的做法更简单，但是结合律的证明是非常冗长乏味的. 这个定义使用起来也更笨拙，因为证明通常要分情况讨论(例如，见例 2.90).

我们现在停止使用记号田，将用

$$[a]+[b]=[a+b]$$

表示$\mathbb{I}_m$ 中同余类的和.

→ **推论 2.104** 阶为 $m\geqslant 2$ 的循环群都和$\mathbb{I}_m$ 同构.

证明 在例 2.90 中，我们已经看到阶相同的两个有限循环群同构. ■

我们现在讨论乘法.

→ **命题 2.105** 函数 μ：$\mathbb{I}_m\times\mathbb{I}_m\to\mathbb{I}_m$，

$$\mu([a],[b])=[ab],$$

是$\mathbb{I}_m$ 上的一个运算. 这个运算满足结合律和交换律，且[1]是单位元. 174

证明 为看出 μ 是(定义良好的)函数，我们必须证明，若$[a]=[a']$和$[b]=[b']$，则$\mu([a],[b])=\mu([a'],[b'])$，即$[ab]=[a'b']$. 但这正是命题 1.60(ii).

仅在这个证明中，我们用⊠表示同余类的乘法：

$$\mu([a],[b])=[a]\boxtimes[b]=[ab].$$

由普通乘法满足结合律得运算⊠满足结合律：

$$
\begin{aligned}
[a]\boxtimes([b]\boxtimes[c])&=[a]\boxtimes[bc]\\
&=[a(bc)]\\
&=[(ab)c]
\end{aligned}
$$

$$=[ab]\boxtimes[c]$$
$$=([a]\boxtimes[b])\boxtimes[c].$$

由普通乘法满足交换律得运算⊠满足交换律：

$$[a]\boxtimes[b]=[ab]=[ba]=[b]\boxtimes[a].$$

单位元是[1]：因为对所有 $a\in\mathbb{Z}$ 有

$$[1]\boxtimes[a]=[1a]=[a].$$ ■

我们现在停止使用记号⊠，将用

$$[a][b]=[ab]$$

表示$\mathbb{I}_m$ 中同余类的积，而不用$[a]\boxtimes[b]$. 注意到，$\mathbb{I}_m$ 在乘法下不作成群，因为有些元素没有逆元，例如[0].

→ **命题 2.106** *(i)若$(a,m)=1$，则关于$[x]$的方程$[a][x]=[b]$在$\mathbb{I}_m$ 中有解.*

(ii)若 p 是素数，则$\mathbb{I}_p$中所有非零元素构成的集合$\mathbb{I}_p^\times$ 是阶为 $p-1$ 的乘法阿贝尔群.

证明 (i)由定理 1.69 知，当$(a,m)=1$ 时，同余方程 $ax\equiv b \bmod m$ 有解，也就是说，当 a 和 m 互素时，关于$[x]$的方程$[a][x]=[b]$在$\mathbb{I}_m$ 中有解.（回忆一下，若 $sa+tm=1$，则$[x]=[sb]$.）

(ii)假设 $m=p$ 是素数. 若 $0<a<p$，则$(a,p)=1$，且由(i)知方程$[a][x]=[1]$在$\mathbb{I}_p$ 中有解，即$[a]$在$\mathbb{I}_p$ 中有逆元. 这样我们就证明了$\mathbb{I}_p^\times$ 是阿贝尔群. 它的阶是 $p-1$，因为它是从$\mathbb{I}_p$
175 中去掉[0]得到的. ■

我们将在定理 3.55 中证明，对每个素数 p，$\mathbb{I}_p^\times$ 是循环群.

我们现在给出费马定理的一个新的证明，它完全不同于前面定理 1.64 所给出的证明.

→ **推论 2.107(费马定理)** *若 p 是素数且$a\in\mathbb{Z}$，则*

$$a^p\equiv a \bmod p.$$

证明 根据命题 2.100，只须证明$\mathbb{I}_p$ 中$[a^p]=[a]$. 若$[a]=[0]$，则由命题 2.105 得$[a^p]=[a]^p=[0]^p=[0]=[a]$. 若$[a]\neq[0]$，则$[a]\in\mathbb{I}_p^\times$，这里$\mathbb{I}_p^\times$ 是$\mathbb{I}_p$ 中非零元素构成的乘法群. 由拉格朗日定理的推论 2.86 知$[a]^{p-1}=[1]$，这是因为$|\mathbb{I}_p^\times|=p-1$. 等式两边乘以$[a]$得到$[a^p]=[a]^p=[a]$. 因此 $a^p\equiv a \bmod p$. ■

注意：若 $m\geqslant 2$ 不是素数，则$\mathbb{I}_m^\times$ 不是群：若 $m=ab$，其中 $1<a, b<m$，则$[a],[b]\in\mathbb{I}_m^\times$，但是它们的积$[a][b]=[ab]=[m]=[0]\notin\mathbb{I}_m^\times$. 我们定义$\mathbb{I}_p^\times$ 的一个类似物，使之能用来推广费马定理.

→ **定义** *设 $U(\mathbb{I}_m)$是$\mathbb{I}_m$ 中所有有逆元的同余类构成的集合，即，若存在$[s]\in\mathbb{I}_m$ 使得$[s][a]=[1]$，则$[a]\in U(\mathbb{I}_m)$.*

→ **引理 2.108** *(i)$U(I_m)=\{[r]\in\mathbb{I}_m:(r,m)=1\}$.*

(ii)$U(I_m)$是阶为 $\phi(m)$的乘法阿贝尔群，其中 $\phi(m)$是欧拉 ϕ-函数.

证明 (i)设 $E=\{[r]\in\mathbb{I}_m:(r,m)=1\}$. 若$[r]\in E$，则$(r,m)=1$，所以存在整数 s 和 t 使得 $sr+tm=1$. 因而 $sr\equiv 1 \bmod m$. 因此$[sr]=[s][r]=[1]$，所以$[r]\in U(I_m)$. 对于反包含，

假设$[r]\in U(I_m)$，即存在$[s]\in U(I_m)$使得$[s][r]=[1]$．但是$[s][r]=[sr]=[1]$，所以$m\mid(sr-1)$，即存在整数t使得$tm=sr-1$．由习题1.56知$(r,m)=1$，所以$[r]\in E$．

(ii)由习题1.58知，由$(r,m)=1=(r',m)$可推出$(rr',m)=1$．因而，由$[r]$，$[r']\in U(\mathbb{I}_m)$推出$[r][r']=[rr']\in U(I_m)$，所以乘法是$U(\mathbb{I}_m)$上的一个运算．命题2.105表明，乘法满足结合律和交换律，且单位元是$[1]$．由命题2.106(i)知，关于$[x]\in\mathbb{I}_m$的方程$[r][x]=[1]$有解，即每个$[r]\in U(I_m)$有逆元．因此$U(I_m)$是阿贝尔群，由命题1.42知，其阶为$|U(\mathbb{I}_m)|=\phi(m)$． ■

若p是素数，则$\phi(p)=p-1$，$U(I_p)=I_p^\times$． 176

→ **定理2.109(欧拉定理)** 若$(r,m)=1$，则

$$r^{\phi(m)}\equiv 1 \bmod m.$$

证明 若G是阶为n的有限群，则由拉格朗日定理的推论2.86知，对所有$x\in G$有$x^n=1$．这里，根据引理2.108，若$[r]\in U(I_m)$，则$[r]^{\phi(m)}=[1]$．用同余记号时，这是说：若$(r,m)=1$，则$r^{\phi(m)}\equiv 1 \bmod m$． ■

例2.110 容易看出

$$U(\mathbb{I}_8)=\{[1],[3],[5],[7]\}\cong \mathbf{V},$$

因为$[3]^2=[9]=[1]$，$[5]^2=[25]=[1]$，$[7]^2=[49]=[1]$．

另外，

$$U(\mathbb{I}_{10})=\{[1],[3],[7],[9]\}\cong \mathbb{I}_4,$$

因为$[3]^4=[81]=[1]$，而$[3]^2=[9]=[-1]\neq[1]$． ◀

→ **定理2.111(威尔逊定理)** *整数p是素数当且仅当*

$$(p-1)!\equiv -1 \bmod p.$$

证明 设p是一个素数．我们可以假设$p\geqslant 3$，因为$1\equiv -1 \bmod 2$．若$a_1,a_2,\cdots,a_n$是有限阿贝尔群G中的所有元素的一个序列，则乘积$a_1a_2\cdots a_n$等于所有满足$a^2=1$的元素a的乘积，这是因为其他元素和它的逆元抵消了．因为$p\geqslant 3$是素数，所以由习题1.88知$\mathbb{I}_p^\times$仅有一个元素阶为2，即$[-1]$．于是$\mathbb{I}_p^\times$中所有元素的乘积$[(p-1)!]$等于$[-1]$．因此$(p-1)!\equiv -1 \bmod p$．

反之，若$(m-1)!\equiv -1 \bmod m$，则$(m,(m-1)!)=1$．假设m是一个合数，则存在整数a满足$a\mid m$，$1<a\leqslant m-1$．因为$a\mid a!$，所以$a\mid(m-1)!$．因此$a>1$是m和$(m-1)!$的公因子，矛盾．因此m是素数． ■

注 像欧拉定理推广了费马定理一样，我们也可以推广威尔逊(Wilson)定理：用$U(\mathbb{I}_n)$代替$U(\mathbb{I}_p)$．例如，我们可以证明，对所有$m\geqslant 3$，$U(\mathbb{I}_{2^m})$恰有3个阶为2的元素，即$[-1]$，$[1+2^{m-1}]$和$[-(1+2^{m-1})]$．于是，所有奇数r的乘积模2^m同余于1，其中$1\leqslant r<2^m$，这是因为

$$\begin{aligned}(-1)(1+2^{m-1})(-1-2^{m-1})&=(1+2^{m-1})^2\\&=1+2^m+2^{2m-2}\equiv 1 \bmod 2^m.\end{aligned}$$ 177

因为同态π：$\mathbb{Z}\to\mathbb{I}_m$，$\pi$：$a\mapsto[a]$是一个满射，所以$\mathbb{I}_m$等于$\operatorname{im}\pi$．因此，$\mathbb{I}_m$中每个元素形如$\pi(a)$，$a\in\mathbb{Z}$，且$\pi(a)+\pi(b)=\pi(a+b)$．根据加法群$\mathbb{Z}$来描述加法群$\mathbb{I}_m$的方法可以推广到任

意群，而不一定是阿贝尔群．假设 $f:G\to H$ 是群 G 和 H 之间的一个满同态．因为 f 是满射，所以 H 中每个元素形如 $f(a)$，$a\in G$，且 H 中的运算是 $f(a)f(b)=f(ab)$，其中 a，$b\in G$．现在 $K=\ker f$ 是 G 的正规子群，我们将单独由 G 和 K 重新构造 $H=\operatorname{im} f$．

设 $\mathcal{S}(G)$ 是群 G 的所有非空子集构成的集合，我们先介绍 $\mathcal{S}(G)$ 上的一个运算．设 X，$Y\in\mathcal{S}(G)$，定义

$$XY=\{xy:x\in X,y\in Y\}.$$

这个乘法满足结合律：$X(YZ)=\{x(yz):x\in X,\ y\in Y,\ z\in Z\}$，$(XY)Z=\{(xy)z:x\in X,\ y\in Y,\ z\in Z\}$，而 G 中结合律成立，所以 $x(yz)=(xy)z$．

这个乘法的一个例子是：单点子集 $\{a\}$ 和子群 $H\leqslant G$ 的乘积是陪集 aH．

第二个例子，若 H 是 G 的子群，则

$$HH=H.$$

因为子群在乘法运算下封闭，所以当 h，$h'\in H$ 时 $hh'\in H$，因此 $HH\subseteq H$．对于反包含，设 $h\in H$，则 $h=h1\in HH$（因为 $1\in H$），因此 $H\subseteq HH$．

在 $\mathcal{S}(G)$ 中，两个子集 X 和 Y 可能满足交换律，即使它们的组成元素不交换．例如，取 $X=Y=H$，这里 H 是 G 的一个非阿贝尔子群．还有一个更有趣的例子：设 $G=S_3$，$K=\langle(1\ 2\ 3)\rangle$．现在 $(1\ 2)$ 不能和 $(1\ 2\ 3)\in K$ 交换，但我们断言 $(1\ 2)K=K(1\ 2)$．

→ **引理 2.112** *群 G 的子群 K 是正规子群当且仅当对每个 $b\in G$ 有 $bK=Kb$.*

证明 设 $bk\in bK$．因为 K 是正规子群，所以 $bkb^{-1}\in K$，不妨设 $bkb^{-1}=k'\in K$，所以 $bk=(bkb^{-1})b=k'b\in Kb$，所以 $bK\subseteq Kb$．对于反包含，设 $kb\in Kb$．因为 K 是正规子群，所以 $(b^{-1})k(b^{-1})^{-1}=b^{-1}kb\in K$，不妨设 $b^{-1}kb=k''\in K$．因而 $kb=b(b^{-1}kb)=bk''\in bK$，$Kb\subseteq bK$．因此，当 $K\lhd G$ 时 $bK=Kb$．

尽管充分性已在习题 2.79 中出现过，但我们还是在这里证明一下．假设对所有 $b\in G$ 有 $bK=Kb$．若 $x\in K$，则 $bx\in bK=Kb$，因而存在 $x'\in K$ 满足 $bx=x'b$，使得 $bxb^{-1}=x'\in K$．因

178 此 $K\lhd G$． ■

由引理 2.112 知，若 $K\lhd G$，则 K 在 G 中的左陪集是 K 在 G 中的右陪集；其逆命题是习题 2.107．

以下是由一个给定群构造一个新群的基本方法．

→ **定理 2.113** *设 G/K 是群 G 的子群 K 的所有陪集构成的族．若 K 是正规子群，则对所有 a，$b\in G$ 有*

$$aKbK=abK,$$

且 G/K 在该运算下作成群.

注 *群 G/K 称为 G 模 K 的商群．若 G 是有限群，则 G/K 的阶 $|G/K|$ 等于指数 $[G:K]=|G|/|K|$（大概，这就是之所以叫商群的原因吧）.*

证明 两个陪集的乘积 $(aK)(bK)$ 可以看作是 $\mathcal{S}(G)$ 中 4 个元素的乘积．因此，根据定理 2.49，半群 $\mathcal{S}(G)$ 中的结合律给出了广义结合律：

$$(aK)(bK) = a(Kb)K = a(bK)K = abKK = abK,$$

这是因为 K 是正规的，所以由引理 2.112 知，对所有 $b\in K$ 有 $Kb=bK$，又因为 K 是子群，所以 $KK=K$. 因此，K 的两个陪集的乘积还是 K 的陪集，因此 G/K 上的运算得到了定义. 因为$\mathcal{S}(G)$中乘法满足结合律，所以等式 $X(YZ)=(XY)Z$ 成立，特别地，当 X，Y，Z 是 K 的陪集时，等式 $X(YZ)=(XY)Z$ 也成立，因此 G/K 上的运算满足结合律. 单位元是陪集 $K=1K$，因为$(1K)(bK)=1bK=bK$. aK 的逆元是 $a^{-1}K$，因为$(a^{-1}K)(aK)=a^{-1}aK=K$. 因此，G/K 是一个群. ■

→ **例 2.114** 我们证明：商群$\mathbb{Z}/\langle m\rangle$正是$\mathbb{I}_m$，其中$\langle m\rangle$是由正整数 m 的所有倍数构成的(循环)子群. 因为$\mathbb{Z}$是阿贝尔群，所以$\langle m\rangle$一定是正规子群. 集合$\mathbb{Z}/\langle m\rangle$和$\mathbb{I}_m$是一样的，因为它们是由相同的元素构成：陪集 $a+\langle m\rangle$是同余类$[a]$：

$$a+\langle m\rangle = \{a+km : k\in \mathbb{Z}\} = [a].$$

它们的运算也是一样的：$\mathbb{Z}/\langle m\rangle$中的加法是

$$(a+\langle m\rangle)+(b+\langle m\rangle) = (a+b)+\langle m\rangle;$$

因为 $a+\langle m\rangle=[a]$，所以上式正是$[a]+[b]=[a+b]$，即是$\mathbb{I}_m$ 中的求和. 因此，$\mathbb{I}_m$ 等于商群 $\mathbb{Z}/\langle m\rangle$. ◀

以下是命题 2.93(ii)的逆命题. 回忆引理 2.82(i)：若 K 是G 的子群，则陪集 aK 和bK 相等当且仅当 $b^{-1}a\in K$. 特别地，若 $b=1$，则 $aK=K$ 当且仅当$a\in K$. 179

→ **推论 2.115** *每个正规子群都是某个同态的核.*

证明 若 $K\lhd G$，则定义**自然映射** $\pi: G\to G/K$，$\pi(a)=aK$. 有了这个记号，公式 $aKbK=abK$ 可重写为 $\pi(a)\pi(b)=\pi(ab)$，因此 π 是一个(满)同态. 因为 K 是G/K 的单位元，所以由引理 2.82(i)知

$$\ker\pi = \{a\in G : \pi(a) = K\} = \{a\in G : aK = K\} = K.$$ ■

下面这个定理告诉我们：每个同态可以产生一个同构，且商群仅是同态的象. 诺特(E. Noether，1882—1935)强调了这个事实的重要性.

→ **定理 2.116(第一同构定理)** *设 $f: G\to H$ 是一个同态，则*

$$\ker f\lhd G \text{ 且 } G/\ker f\cong \operatorname{im} f.$$

具体地讲，若 $\ker f=K$，则函数 $\varphi: G/K\to \operatorname{im} f\leqslant H$，$\varphi$: $aK\mapsto f(a)$是一个同构.

证明 在命题 2.93(ii)中我们已经看到，$K=\ker f$ 是 G 的正规子群. φ 是定义良好的：若 $aK=bK$，则存在 $k\in K$ 使得 $a=bk$，又因为 $f(k)=1$，所以 $f(a)=f(bk)=f(b)f(k)=f(b)$.

现在证明 φ 是一个同态. 因为 f 是同态且 $\varphi(aK)=f(a)$，所以

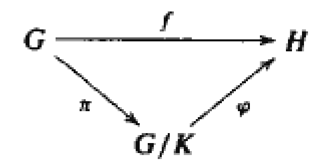
$$\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK).$$

显然 $\operatorname{im}\varphi\leqslant\operatorname{im} f$. 对于反包含，注意到若 $y\in\operatorname{im} f$，则存在 $a\in G$ 使 $y=f(a)$，所以 $y=f(a)=\varphi(aK)$. 因此 φ 是满射.

最后，证明 φ 是单射. 设 $\varphi(aK)=\varphi(bK)$，则 $f(a)=f(b)$，则 $1=f(b)^{-1}f(a)=f(b^{-1}a)$，因此 $b^{-1}a\in\ker f=K$，由引理 2.82(i)知 $aK=bK$，所以 φ 是单射. 因此 $\varphi: G/K\to \operatorname{im} f$ 是一个同构. ■

注 *右图描绘了第一同构定理的证明，其中 $\pi: G \to G/K$，$\pi: a \mapsto aK$ 是自然映射.*

180 给定同态 $f: G \to H$，我们应当立即去求它的核和象，第一同构定理进一步给出一个同构 $G/\ker f \cong \operatorname{im} f$. 因为同构的群之间没有太大的区别，所以第一同构定理还说明了商群和同态象之间没有很大的区别.



例 2.117 我们再看一下例 2.90，它证明了任意两个阶为 m 的循环群是同构的. 设 $G=\langle a\rangle$ 是阶为 m 的循环群，则定义一个同态 $f: \mathbb{Z} \to G$，对所有 $n \in \mathbb{Z}$ 有 $f(n)=a^n$. f 是满射(因为 a 是 G 的生成元)，由引理 2.53 知 $\ker f=\{n \in \mathbb{Z}: a^n=1\}=\langle m\rangle$. 第一同构定理给出一个同构 $\mathbb{Z}/\langle m\rangle \cong G$. 这样，我们证明了阶为 m 的循环群和 $\mathbb{Z}/\langle m\rangle$ 同构，因此任意两个阶为 m 的循环群相互同构. 因为例 2.114 表明 $\mathbb{Z}/\langle m\rangle=\mathbb{I}_m$，所以阶为 m 的循环群和 $\mathbb{I}_m$ 同构. ◀

例 2.118 商群 $\mathbb{R}/\mathbb{Z}$ 是怎样的？定义 $f: \mathbb{R} \to S^1$ 为

$$f: x \mapsto e^{2\pi i x},$$

其中 S^1 是圆群. 由正弦和余弦的加法公式知 f 是一个同态，即 $f(x+y)=f(x)f(y)$. 映射 f 是满射，且 $\ker f=\{x \in \mathbb{R}: e^{2\pi i x}=\cos 2\pi x+i\sin 2\pi x=1\}$. 显然，$\mathbb{Z} \subseteq \ker f$，这是因为若 $n \in \mathbb{Z}$，则 $f(n)=e^{2\pi i n}=1$. 对于反包含，若 $1=f(x)=e^{2\pi i x}$，则 $\cos 2\pi x=0=\sin 2\pi x$ 迫使 x 是一个整数. 因此 $\ker f=\mathbb{Z}$，且由第一同构定理知

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$ ◀

我们很自然地会问：当 H 和 K 都是子群时，HK 是否还是子群？一般地，HK 不一定是子群. 例如，设 $G=S_3$，$H=\langle(1\ 2)\rangle$，$K=\langle(1\ 3)\rangle$，则

$$HK=\{(1),(1\ 2),(1\ 3),(1\ 3\ 2)\}$$

不是子群，否则与拉格朗日定理矛盾. 习题 2.106 给出了子群 H 和 K 的积 HK 仍为子群的一个必要充分条件.

命题 2.119 *(i)若 H 和 K 是群 G 的子群且其中一个是正规子群，则 HK 是 G 的子群，并且 $HK=KH$.*

181 *(ii)若 H 和 K 都是正规子群，则 HK 也是正规子群.*

证明 (i)首先不妨设 $K \lhd G$. 我们断言 $HK=KH$. 因为 $K \lhd G$，若 $hk \in HK$，则 $k'=hkh^{-1} \in K$，且

$$hk=hkh^{-1}h=k'h \in KH.$$

因此，$HK \subseteq KH$. 对于反包含，则应是 $kh=hh^{-1}kh=hk'' \in HK$.（注意，当 $H \lhd G$ 时，可以用同样的方法证明 $HK=KH$.）

现在证明 HK 是子群. 因为 $1 \in H$ 且 $1 \in K$，所以 $1=1 \cdot 1 \in HK$. 若 $hk \in HK$，则 $(hk)^{-1}=k^{-1}h^{-1} \in KH=HK$. 若 hk，$h_1k_1 \in HK$，则 $h_1^{-1}kh_1=k' \in K$，且

$$hkh_1k_1=hh_1(h_1^{-1}kh_1)k_1=(hh_1)(k'k_1) \in HK.$$

因此，HK 是 G 的子群.

(ii)若 $g \in G$，则

$$ghkg^{-1}=(ghg^{-1})(gkg^{-1}) \in HK.$$

因此，$HK \lhd G$. ■

以下是一个有用的计数结果.

命题 2.120(乘积公式) 设 H，K 是有限群 G 的子群，则

$$|HK||H\cap K|=|H||K|,$$

其中 $HK=\{hk: h\in H, k\in K\}$.

注 因为我们没有假设 H 或 K 是正规子群，所以子集 HK 不一定是子群.

证明 定义函数 $f: H\times K\to HK$，$f:(h,k)\mapsto hk$. 显然，f 是满射. 只需证明：对每个 $x\in HK$ 有 $|f^{-1}(x)|=|H\cap K|$，其中 $f^{-1}(x)=\{(h,k)\in H\times K: f(h,k)=x\}$ $\Big[$因为 $H\times K$ 是无交并 $\bigcup_{x\in HK} f^{-1}(x)$，其阶为 $|HK||H\cap K|\Big]$.

我们断言，若 $x=hk$，则

$$f^{-1}(x)=\{(hd,d^{-1}k): d\in H\cap K\}.$$

每个 $(hd, d^{-1}k)\in f^{-1}(x)$，这是因为 $f(hd, d^{-1}k)=hdd^{-1}k=hk=x$. 对于反包含，设 $(h', k')\in f^{-1}(x)$，则 $h'k'=hk$，因此 $h^{-1}h'=kk'^{-1}\in H\cap K$，称这个元素为 d，则 $h'=hd$，$k'=d^{-1}k$，所以 (h', k') 属于等式右边. 因此，

$$|f^{-1}(x)|=|\{(hd,d^{-1}k): d\in H\cap K\}|=|H\cap K|,$$

因为 $d\mapsto(hd, d^{-1}k)$ 是一个双射. ■

下面的两个结果是第一同构定理的变形. [182]

→ **定理 2.121(第二同构定理)** 若 H 和 K 都是群 G 的子群，$H\lhd G$，则 HK 是子群，$H\cap K\lhd K$，且

$$K/(H\cap K)\cong HK/H.$$

证明 我们先证明 HK/H 是有意义的，然后描述其元素. 由于 $H\lhd G$，命题 2.119 表明 HK 是子群. 从一个更一般的事实中可得 H 在 HK 中的正规性：若 $H\leqslant S\leqslant G$ 且 H 在 G 中正规，则 H 在 S 中正规(若对每个 $g\in G$ 有 $ghg^{-1}\in H$，则对每个 $g\in S$ 有 $ghg^{-1}\in H$).

我们现在证明每个陪集 $xH\in HK/H$ 有形式 kH，$k\in K$. 当然，$xH=hkH$，其中 $h\in H$，$k\in K$. 但是对某个 $h'\in H$ 有 $hk=k(k^{-1}hk)=kh'$，所以 $hkH=kh'H=kH$.

于是函数 $f: K\to HK/H$，$f: k\mapsto kH$，是满射. 另外，f 是一个同态，因为它是自然映射 $\pi: G\to G/H$ 的限制. 由于 $\ker\pi=H$，所以 $\ker f=H\cap K$，所以 $H\cap K$ 是 K 的正规子群. 由第一同构定理知 $K/(H\cap K)\cong HK/H$. ■

当有一个子群是正规子群时，第二同构定理给出了该特殊情形时的乘积公式：若 $K/(H\cap K)\cong HK/H$，则 $|K/(H\cap K)|=|HK/H|$，所以 $|HK||H\cap K|=|H||K|$.

→ **定理 2.122(第三同构定理)** 若 H 和 K 都是群 G 的正规子群，$K\leqslant H$，则 $H/K\lhd G/K$，且

$$(G/K)/(H/K)\cong G/H.$$

证明 定义 $f: G/K\to G/H$，$aK\mapsto aH$. 注意到 f 是一个(定义良好的)函数，因为若 $a'\in G$ 和 $a'K=aK$，则 $a^{-1}a'\in K\leqslant H$，所以 $aH=a'H$. 容易看出 f 是满同态.

因为 $aK=H$ 当且仅当 $a\in H$，所以 $\ker f=H/K$，所以 H/K 是 G/K 的正规子群. 由于 f 是满射，由第一同构定理知 $(G/K)/(H/K)\cong G/H$. ■

第三同构定理是容易记住的：分式 $(G/K)/(H/K)$ 中的 K 可以约去. 在证明了第三同构定理之后，我们就能更好地欣赏第一同构定理了. $(G/K)/(H/K)$ 的元素是 H/K 的陪集，这些陪集的代表元本身是陪集 (G/K) 的. 第三同构定理的直接证明是令人厌烦的.

下面这个结果描述了商群 G/K 的子群，它可以看作是第四同构定理. 回忆一下，利用直接象和逆象，函数 $f: X\to Y$ 在 X 的子集和 Y 的子集之间建立联系. 我们现在把这个观点应用
183 到 $f: G\to H$ 是同态这一特殊情形中.

若 G 是一个群，且 $K\lhd G$，则设 $\mathbf{Sub}(G;K)$ 表示 G 的包含 K 的所有子群 S 构成的族，设 $\mathbf{Sub}(G/K)$ 表示 G/K 的所有子群构成的族.

→ **命题 2.123（对应定理）** *设 G 是一个群，$K\lhd G$.*

(i) 函数 $\mathbf{Sub}(G;K)\to\mathbf{Sub}(G/K)$，$S\mapsto S/K$ 是双射.

(ii) 记 S/K 为 S^*，则 $\mathbf{Sub}(G;K)$ 中 $T\leqslant S\leqslant G$ 当且仅当 $\mathbf{Sub}(G/K)$ 中 $T^*\leqslant S^*$，此时 $[S:T]=[S^*:T^*]$.

(iii) $\mathbf{Sub}(G;K)$ 中 $T\lhd S$ 当且仅当 $\mathbf{Sub}(G/K)$ 中 $T^*\lhd S^*$，此时 $S/T\cong S^*/T^*$.

证明 (i) 设 $\Phi:\mathbf{Sub}(G;K)\to\mathbf{Sub}(G/K)$ 表示函数 $\Phi: S\mapsto S/K$（用常规方法检验：若 S 是 G 的包含 K 的子群则 S/K 是 G/K 的子群）.

为看出 Φ 是单射，我们先证明若 $K\leqslant S\leqslant G$ 则 $\pi^{-1}\pi(S)=S$，其中 $\pi: G\to G/K$ 是自然映射. 和通常一样，根据命题 2.14(iii)，有 $S\leqslant\pi^{-1}\pi(S)$. 对于反包含，设 $a\in\pi^{-1}\pi(S)$，则存在 $s\in S$ 有 $\pi(a)=\pi(s)$. 于是 $as^{-1}\in\ker\pi=K$，所以存在 $k\in K$ 有 $a=sk$. 但是 $K\leqslant S$，所以 $a=sk\in S$.

现在假设 $\pi(S)=\pi(S')$，其中 S 和 S' 都是 G 的包含 K 的子群（注意 $\pi(S)=S/K$），则 $\pi^{-1}\pi(S)=\pi^{-1}\pi(S')$，所以 $S=S'$，因而 Φ 是单射.

为看出 Φ 是满射，设 U 是 G/K 的子群. 根据例 2.92(iv)，$\pi^{-1}(U)$ 是 G 的包含 $K=\pi^{-1}(\{1\})$ 的子群，且根据命题 2.14(ii) 知 $\pi(\pi^{-1}(U))=U$.

(ii) 命题 2.14(*i*) 表明由 $T\leqslant S\leqslant G$ 可以推出 $T/K=\pi(T)\leqslant\pi(S)=S/K$. 反之，假设 $T/K\leqslant S/K$. 若 $t\in T$，则 $tK\in T/K\leqslant S/K$，所以存在 $s\in S$ 有 $tK=sK$. 因而存在 $k\in K\leqslant S$ 可使得 $t=sk$，所以 $t\in S$.

对于 G 是有限群这一重要的特殊情形，我们证明 $[S:T]=[S^*:T^*]$ 如下：

$$\begin{aligned}[S^*:T^*]&=|S^*|/|T^*|\\&=|S/K|/|T/K|\\&=(|S|/|K|)/(|T|/|K|)\\&=|S|/|T|\\&=[S:T].\end{aligned}$$

184 为证明 $[S:T]=[S^*:T^*]$ 在一般情形中成立，只需证明形如 sT 的所有陪集构成的族和形如 s^*T^* 的所有陪集构成的族之间存在一个双射，其中 $s\in S$，$s^*\in S^*$. 读者可以验证 $sT\mapsto\pi(s)T^*$ 是这样的双射.

(iii)第三同构定理表明，若 $T\lhd S$，则 $T/K\lhd S/K$ 和 $(S/K)/(T/K)\cong S/T$，即 $S^*/T^*\cong S/T$. 还要证明若 $T^*\lhd S^*$ 则 $T\lhd S$，即若 $t\in T$ 和 $s\in S$ 则 $sts^{-1}\in T$. 现在

$$\pi(sts^{-1})=\pi(s)\pi(t)\pi(s)^{-1}\in\pi(s)T^*\pi(s)^{-1}=T^*,$$

所以 $sts^{-1}\in\pi^{-1}(T^*)=T$. ■

对待商群时，我们通常会说 G/K 的每个子群有 S/K 的形式，其中 $S\leqslant G$ 是包含 K 的唯一子群，而不明显地提到对应定理.

→ **命题 2.124** (i)若 G 是有限阿贝尔群，p 是 $|G|$ 的素因子，则 G 含有阶为 p 的元素.

(ii)若 G 是有限阿贝尔群，则对 $|G|$ 的每个因子 d，G 有阶为 d 的子群.

证明 (i)我们对 $n=|G|$ 应用归纳法证明，若 p 是 $|G|$ 的素因子，则 G 中存在阶为 p 的元素. 基础步骤 $n=1$ 成立，因为 1 不存在素因子. 对于归纳步骤，选取阶为 $k>1$ 的元素 $a\in G$. 若 $p\mid k$，不妨设 $k=p\ell$，则习题 2.40 是说 a^{ℓ} 的阶为 p. 若 $p\nmid k$，则考虑循环子群 $H=\langle a\rangle$. 因为 G 是阿贝尔群，所以 $H\lhd G$，所以商群 G/H 存在. 注意 $|G/H|=n/k$ 被 p 整除，所以由归纳假设知存在阶为 p 的元素 $bH\in G/H$. 若 b 的阶为 m，则 G/H 中有 $(bH)^m=b^mH=H$，所以由引理 2.53 得 $p\mid m$. 我们回到了第一种情形.

(ii)现在对 $d\geqslant 1$ 应用归纳法证明一般结果. 基础步骤 $d=1$ 显然成立，所以我们可假设 $d>1$，即可假设 d 有一个素因子，不妨设为 p. 根据归纳法，G 含有一个阶为 p 的子群 H. 因为 G 是阿贝尔群，$H\lhd G$，所以商群 G/H 有定义. 另外，$|G/H|=|G|/p$，所以 $(d/p)\mid |G/H|$. 由归纳假设知存在子群 $S^*\leqslant G/H$ 满足 $|S^*|=d/p$. 根据对应定理，存在一个中间子群 S(即 $H\leqslant S\leqslant G$)满足 $S^*=S/H$. 因此 $|S|=p|S^*|=p\cdot(d/p)=d$. ■

命题 2.124 的(i)推广了柯西定理，即定理 2.147，该定理是说：若 p 是 $|G|$ 的素因子，其中 G 是任意有限群，不必是阿贝尔群，则 G 有阶为 p 的元素. 但是(ii)一般情况下不成立：命题 2.99 表明，A_4 是阶为 12 的群，但没有阶为 6 的子群.

以下是由两个给定的群构造一个新群的另一种方法. 185

→ **定义** 若 H 和 K 都是群，则它们的**直积**，记为 $H\times K$，是由所有有序对 (h,k) 构成的集合，其中 $h\in H$，$k\in K$，带上运算：

$$(h,k)(h',k')=(hh',kk').$$

验证 $H\times K$ 是群[单位元是 $(1,1)$ 且 $(h,k)^{-1}=(h^{-1},k^{-1})$]是常规的. 注意 $H\times K$ 是阿贝尔群当且仅当 H 和 K 都是阿贝尔群.

→ **例 2.125** 四元群 $\mathbf{V}$ 与 $\mathbb{I}_2\times\mathbb{I}_2$ 同构. 读者可以验证函数 $f:\mathbf{V}\to\mathbb{I}_2\times\mathbb{I}_2$ 是一个同构，其定义为

$$\begin{aligned}f:(1)&\mapsto([0],[0]),\\ f:(1\ 2)(3\ 4)&\mapsto([1],[0]),\\ f:(1\ 3)(2\ 4)&\mapsto([0],[1]),\\ f:(1\ 4)(2\ 3)&\mapsto([1],[1]).\end{aligned}$$ ◀

我们现在对直积应用第一同构定理.

→ **命题 2.126** 设 G 和 G' 都是群，$K\lhd G$ 和 $K'\lhd G'$ 都是正规子群. 则 $K\times K'$ 是 $G\times G'$ 的正

规子群，且存在同构

$$(G\times G')/(K\times K')\cong (G/K)\times (G'/K').$$

证明 设 $\pi: G\to G/K$ 和 $\pi': G'\to G'/K'$ 都是自然映射. 读者可以验证 $f: G\times G'\to (G/K)\times (G'/K')$,

$$f:(g,g')\mapsto(\pi(g),\pi'(g'))=(gK,g'K')$$

是一个满同态，且满足 $\ker f=K\times K'$. 由第一同构定理得到了我们想要的同构. ■

以下是直积的一个性质.

→ **命题 2.127** *若 G 是包含正规子群 H 和 K 的群，满足 $H\cap K=\{1\}$ 和 $HK=G$，则 $G\cong H\times K$.*

证明 若 $g\in G=HK$，则 $g=hk$，其中 $h\in H$，$k\in K$. 我们先证明，若 $g\in G$，则分解式 $g=hk$ 是唯一的. 若 $hk=h'k'$，则 $h'^{-1}h=k'k^{-1}\in H\cap K=\{1\}$. 因此 $h'=h$，$k'=k$. 现在可以定义函数 $\varphi: G\to H\times K$，$\varphi(g)=(h, k)$，其中 $g=hk$，$h\in H$，$k\in K$. 为看出 φ 是否是同态，
186 设 $g'=h'k'$，所以 $gg'=hkh'k'=hh'kk'$. 因而 $\varphi(gg')=\varphi(hkh'k')$，这个式子不方便计算. 假设我们知道了若 $h\in H$ 和 $k\in K$ 则 $hk=kh$，则可以继续得：

$$\begin{aligned}\varphi(hkh'k')&=\varphi(hh'kk')\\&=(hh',kk')\\&=(h,k)(h',k')\\&=\varphi(g)\varphi(g').\end{aligned}$$

设 $h\in H$，$k\in K$. 由于 $K\lhd G$，所以 $hkh^{-1}\in K$，所以 $(hkh^{-1})k^{-1}\in K$. 由于 $H\lhd G$，所以 $kh^{-1}k^{-1}\in H$，所以 $h(kh^{-1}k^{-1})\in H$. 但是 $H\cap K=\{1\}$，所以 $hkh^{-1}k^{-1}=1$，$hk=kh$.

现在 φ 是满射，因为若 $(h, k)\in H\times K$，则元素 $g=hk\in G$ 满足 $\varphi(g)=(h, k)$. 最后，若 $\varphi(g)=(1, 1)$，则 $g=hk$，其中 $h=1=k$，所以 $g=1$. 因而 $\ker\varphi=\{1\}$，φ 是单射. 因此 φ 是一个同构. ■

命题 2.127 中的所有条件都是必需的. 例如，设 $G=S_3$，$H=\langle(1\ 2\ 3)\rangle$，$K=\langle(1\ 2)\rangle$，则 $S_3=HK$，$\{1\}=H\cap K$，$H\lhd S_3$，但是 K 不是正规子群. $S_3\cong H\times K$ 不成立，因为 S_3 不是阿贝尔群，而阿贝尔群的直积 $H\times K$ 是阿贝尔群.

→ **定理 2.128** *若 m 和 n 互素，则*

$$\mathbb{I}_{mn}\cong\mathbb{I}_m\times\mathbb{I}_n.$$

证明 我们记 $\mathbb{I}_m$ 和 $\mathbb{I}_n$ 的元素分别为 $[a]_m$ 和 $[a]_n$. 容易证明 $f:\mathbb{Z}\to\mathbb{I}_m\times\mathbb{I}_n$，$f(a)=([a]_m, [a]_n)$，是一个同态. 我们断言 f 是一个满射. 若 $([b]_m, [c]_n)\in\mathbb{I}_m\times\mathbb{I}_n$，则应用中国剩余定理（因为 m 和 n 互素）知，存在整数 a 满足 $([b]_m, [c]_n)=([a]_m, [a]_n)=f(a)$. 现在 $a\in\ker f$ 当且仅当 $a\in\langle m\rangle\cap\langle n\rangle$. 但是，命题 2.80 是说 $\langle m\rangle\cap\langle n\rangle=\langle\ell\rangle$，其中 $\ell=\mathrm{lcm}\{m, n\}$. 根据命题 1.56 知，由 m 和 n 互素得 $\mathrm{lcm}\{m, n\}=mn$，所以 $\ker f=\langle mn\rangle$. 根据第一同构定理，函数 $g:\mathbb{Z}/\langle mn\rangle\to(\mathbb{Z}/\langle m\rangle)\times(\mathbb{Z}/\langle n\rangle)$，$g:[a]_{mn}\mapsto f(a)=([a]_m, [a]_n)$，是一个同构. 因此 $\mathbb{I}_{mn}\cong\mathbb{I}_m\times\mathbb{I}_n$. ■

例如，有 $\mathbb{I}_6\cong\mathbb{I}_2\times\mathbb{I}_3$. 注意，若 m 和 n 不互素，则不存在同构. 例 2.125 表明 $\mathbf{V}\cong\mathbb{I}_2\times\mathbb{I}_2$，但 $\mathbf{V}$ 与 $\mathbb{I}_4$ 不同构，因为 $\mathbf{V}$ 没有阶为 4 的元素.

根据命题 2.74，若 $a\in G$ 且 $\langle a\rangle\cong\mathbb{I}_n$，则 a 的阶为 n. 现在定理 2.128 可以说成是：若元素 a 和 b 交换且它们的阶 m 和 n 互素，则 ab 的阶为 mn. 让我们给出这个结果的直接证明. 187

命题 2.129 *设 G 是群，元素 a，$b\in G$ 交换且阶分别为 m 和 n. 若 $(m, n)=1$，则 ab 的阶为 mn.*

证明 由于 a 和 b 交换，所以对所有 r 有 $(ab)^r=a^rb^r$，所以 $(ab)^{mn}=a^{mn}b^{mn}=1$. 只需证明，若 $(ab)^k=1$，则 $mn\mid k$. 若 $1=(ab)^k=a^kb^k$，则 $a^k=b^{-k}$. 由于 a 的阶为 m，所以有 $1=a^{mk}=b^{-mk}$. 由于 b 的阶为 n，由引理 2.53 得 $n\mid mk$. 因为 $(m, n)=1$，所以由推论 1.40 得 $n\mid k$. 类似的讨论得 $m\mid k$. 最后，习题 1.60 表明 $mn\mid k$. 因此 $mn\leqslant k$，mn 是 ab 的阶. ■

以下是命题 2.75 的变形.

→ **命题 2.130** *若 G 是一个有限阿贝尔群，对 $|G|$ 的每个素因子 p 有唯一的阶为 p 的子群，则 G 是循环群.*

证明 选取阶(不妨设为 n)最大的元素 $a\in G$. 若 p 是 $|G|$ 的一个素因子，则设 $C=C_p$ 是 G 的阶为 p 的唯一子群. 子群 C 一定是循环群，不妨设 $C=\langle c\rangle$. 我们通过证明 $c\in\langle a\rangle$(因而 $C\leqslant\langle a\rangle$)来证明 $p\mid n$. 若 $(p, n)=1$，根据命题 2.129，则 ca 的阶为 $pn>n$，与 a 是阶最大的元素矛盾. 若 $p\mid n$，不妨设 $n=pq$，则 a^q 的阶为 p，因而它位于唯一的阶为 p 的子群 $\langle c\rangle$ 中. 因此，对某个 i 有 $a^q=c^i$. 现在 $(i, p)=1$，所以存在整数 u 和 v 使得 $1=ui+vp$，因而 $c=c^{ui+vp}=c^{ui}c^{vp}=c^{ui}$. 因此，$a^{qu}=c^{ui}=c$，所以 $c\in\langle a\rangle$. 于是 $\langle a\rangle$ 含有满足 $x^p=1$ 的每个元素 $x\in G$.

若 $\langle a\rangle=G$，则我们证完了. 因此，我们可以假设存在 $b\in G$ 满足 $b\notin\langle a\rangle$. 现在 $b^{|G|}=1\in\langle a\rangle$. 设 k 是满足 $b^k\in\langle a\rangle$ 的最小正整数：

$$b^k=a^q.$$

注意 $k\mid |G|$，因为 k 是 $G/\langle a\rangle$ 中 $b\langle a\rangle$ 的阶. 当然，$k\neq 1$，所以存在分解式 $k=pm$，其中 p 是素数. 现在有两种可能. 若 $p\mid q$，则 $q=pu$ 且

$$b^{pm}=b^k=a^q=a^{pu}.$$

因而 $(b^ma^{-u})^p=1$，所以 $b^ma^{-u}\in\langle a\rangle$. 因此 $b^m\in\langle a\rangle$，这与 k 是满足这种性质的最小指数矛盾. 第二种可能是 $p\nmid q$，此时 $(p, q)=1$. 因为存在整数 s 和 t 使得 $1=sp+tq$，所以

$$a=a^{sp+tq}=a^{sp}a^{tq}=a^{sp}b^{pmt}=(a^sb^{mt})^p.$$

因此 $a=x^p$，其中 $x=a^sb^{mt}$，因为 $p\mid n$，所以可以应用习题 2.41，习题 2.41 是说 x 的阶比 a 的阶更大，矛盾. 我们得 $G=\langle a\rangle$. ■ 188

命题 2.130 对非阿贝尔群不成立，因为四元数群 $\mathbf{Q}$ 就是一个反例；它是阶为 8 的非循环群，有唯一的阶为 2 的子群.

以下是直积在数论方面的应用.

→ **推论 2.131** *若 $(m, n)=1$，则 $\phi(mn)=\phi(m)\phi(n)$，其中 ϕ 是欧拉 ϕ-函数.*

证明[⊖] 因为 m 和 n 互素，所以定理 2.128 的证明表明，$g: \mathbb{Z}/\langle mn\rangle\to(\mathbb{Z}/\langle m\rangle)\times(\mathbb{Z}/\langle n\rangle)$，$g: [a]_{mn}\mapsto([a]_m, [a]_n)$，是一个同构. 若 $U(\mathbb{I}_m)=\{[r]\in\mathbb{I}_m: (r, m)=1\}$，则由

⊖ 计算较少的证明见习题 3.54(iii)

引理 2.108 知 $|U(\mathbb{I}_m)|=\phi(m)$. 因此，若我们证明了 $g(U(\mathbb{I}_{mn}))=U(\mathbb{I}_m)\times U(\mathbb{I}_n)$，则有

$$\phi(mn)=|U(\mathbb{I}_{mn})|=|g(U(\mathbb{I}_{mn}))|$$
$$=|U(\mathbb{I}_m)\times U(\mathbb{I}_n)|=|U(\mathbb{I}_m)|\cdot|U(\mathbb{I}_n)|=\phi(m)\phi(n).$$

我们断言 $g(U(\mathbb{I}_{mn}))=U(\mathbb{I}_m)\times U(\mathbb{I}_n)$. 若 $[a]_{mn}\in U(\mathbb{I}_{mn})$，则存在 $[b]_{mn}\in\mathbb{I}_{mn}$ 使得 $[a]_{mn}[b]_{mn}=[1]_{mn}$，且

$$g([ab]_{mn})=([ab]_m,[ab]_n)=([a]_m[b]_m,[a]_n[b]_n)$$
$$=([a]_m,[a]_n)([b]_m,[b]_n)=([1]_m,[1]_n).$$

因而，$[1]_m=[a]_m[b]_m$，$[1]_n=[a]_n[b]_n$，所以 $g([a]_{mn})=([a]_m,\ [a]_n)\in U(\mathbb{I}_m)\times U(\mathbb{I}_n)$，$g(U(\mathbb{I}_{mn}))\leqslant U(\mathbb{I}_m)\times U(\mathbb{I}_n)$.

对于反包含，若 $g([c]_{mn})=([c]_m,\ [c]_n)\in U(\mathbb{I}_m)\times U(\mathbb{I}_n)$，则我们必须证明 $[c]_{mn}\in U(\mathbb{I}_{mn})$. 存在 $[d]_m\in\mathbb{I}_m$ 满足 $[c]_m[d]_m=[1]_m$，存在 $[e]_n\in\mathbb{I}_n$ 满足 $[c]_n[e]_n=[1]_n$. 因为 g 是满射，所以存在 $b\in\mathbb{Z}$ 满足 $([b]_m,\ [b]_n)=([d]_m,\ [e]_n)$，所以

$$g([1]_{mn})=([1]_m,[1]_n)=([c]_m[b]_m,[c]_n[b]_n)=g([c]_{mn}[b]_{mn}).$$

因为 g 是单射，所以 $[1]_{mn}=[c]_{mn}[b]_{mn}$，因此 $[c]_{mn}\in U(\mathbb{I}_{mn})$. ■

现在定义几个群的直积.

→ **定义** 设 H_1，…，H_n 都是群，则它们的**直积**

$$H_1\times\cdots\times H_n$$

是所有 n 元组 $(h_1,\ \cdots,\ h_n)$ 构成的集合，其中对所有 i 有 $h_i\in H_i$，带有两两坐标乘积运算：

$$(h_1,\cdots,h_n)(h_1',\cdots,h_n')=(h_1h_1',\cdots,h_nh_n').$$

189 基本定理即定理 6.11 是说，每个有限阿贝尔群是一些循环群的直积.

习题

H 2.95 判断对错并说明理由.

(i) 若 $\mathbb{I}_m$ 中 $[a]=[b]$，则 $\mathbb{Z}$ 中 $a=b$.

(ii) $\mathbb{I}_m\to\mathbb{Z}$，$[a]\mapsto a$，是一个同态.

(iii) 若 $\mathbb{Z}$ 中 $a=b$，则 $\mathbb{I}_m$ 中 $[a]=[b]$.

(iv) 若 G 是群且 $K\lhd G$，则存在核为 K 的同态 $G\to G/K$.

(v) 若 G 是群且 $K\lhd G$，则每个同态 $G\to G/K$ 的核都是 K.

(vi) 阿贝尔群的商群都是阿贝尔群.

(vii) 若 G，H 都是阿贝尔群，则 $G\times H$ 是阿贝尔群.

(viii) 若 G，H 都是循环群，则 $G\times H$ 是循环群.

(ix) 若群 G 的每个子群都是正规子群，则 G 是阿贝尔群.

(x) 若 G 是群，则 $\{1\}\lhd G$ 和 $G/\{1\}\cong G$.

2.96 证明 $U(\mathbb{I}_9)\cong\mathbb{I}_6$ 和 $U(\mathbb{I}_{15})\cong\mathbb{I}_4\times\mathbb{I}_2$.

2.97 (i) 若 H，K 都是群，不用第一同构定理，证明 $H^*=\{(h,\ 1):h\in H\}$ 和 $K^*=\{(1,\ k):k\in K\}$ 都是 $H\times K$ 的正规子群，并且 $H\cong H^*$ 和 $K\cong K^*$.

(ii) 不用第一同构定理，证明 $f:H\to(H\times K)/K^*$，$f(h)=(h,\ 1)K^*$，是一个同构.

H (iii) 利用第一同构定理证明 $K^*\lhd(H\times K)$ 和 $(H\times K)/K^*\cong H$.

*H 2.98　若 G 是群且 $G/Z(G)$ 是循环群，其中 $Z(G)$ 表示 G 的中心，证明 G 是阿贝尔群，即 $G=Z(G)$. 由此得出，若 G 不是阿贝尔群，则 $G/Z(G)$ 不是循环群.

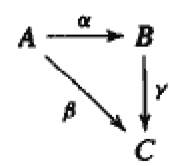
*H 2.99　设 G 是有限群，p 是素数，H 是 G 的正规子群. 证明，若 $|H|$ 和 $|G/H|$ 都是 p 的幂，则 $|G|$ 是 p 的幂.

H 2.100　称群 G 是**有限生成的**，若存在一个有限子集 $X\subseteq G$ 满足 $G=\langle X\rangle$. 证明，有限生成的阿贝尔群 G 的每个子群本身是有限生成的.（若 G 不是阿贝尔群，则此命题不成立.）

*2.101　(i)设 $\pi: G\to H$ 是一个满同态，且 $\ker\pi=T$. 设 $H=\langle X\rangle$，且对每个 $x\in X$，选取元素 $g_x\in G$ 使得 $\pi(g_x)=x$. 证明 G 是由 $T\cup\{g_x: x\in X\}$ 生成的.

(ii)设 G 是群且 $T\lhd G$. 若 T 和 G/T 都是有限生成的，证明 G 也是有限生成的.

*2.102　设 A，B，C 都是群，α，β，γ 都是同态且 $\gamma\circ\alpha=\beta$. 若 α 是满同态，证明 $\ker\gamma=\alpha(\ker\beta)$.



2.103　设 A，B 都是群，$A'\lhd A$ 和 $B'\lhd B$ 都是正规子群，$\alpha: A\to B$ 是一个同态且满足 $\alpha(A')\leqslant B'$. 190

(i)证明 $\alpha_*: A/A'\to B/B'$，$\alpha_*: aA'\mapsto\alpha(a)B'$，是一个定义良好的同态.

(ii)证明，若 α 是满同态，则 α_* 是满同态.

(iii)举一个例子，α 是单同态，而 α_* 不是.

2.104　(i)证明 $\mathbf{Q}/Z(\mathbf{Q})\cong\mathbf{V}$，其中 $\mathbf{Q}$ 是四元数群，$\mathbf{V}$ 是四元群. 由此得出，一个非阿贝尔群通过它的中心得到的商群可以是阿贝尔群.

(ii)证明 $\mathbf{Q}$ 没有和 $\mathbf{V}$ 同构的子群. 由此得出，商群 $\mathbf{Q}/Z(\mathbf{Q})$ 与 $\mathbf{Q}$ 的子群不同构.

H 2.105　设 G 是有限群且 $K\lhd G$. 若 $(|K|,[G:K])=1$，证明 K 是 G 的阶为 $|K|$ 的唯一子群.

*2.106　设 H，K 都是群 G 的子群.

H (i)证明 HK 是 G 的子群当且仅当 $HK=KH$. 特别地，若对所有 $h\in H$ 和 $k\in K$ 有 $hk=kh$，则条件成立.

(ii)若 $HK=KH$ 且 $H\cap K=\{1\}$，证明 $HK\cong H\times K$.

*2.107　证明引理 2.112 的逆命题：若 K 是群 G 的子群，且每个左陪集 aK 等于一个右陪集 Kb，则 $K\lhd G$.

2.108　设 G 是群，并把 $G\times G$ 看作是 G 和自身的直积. 若乘法 $\mu: G\times G\to G$ 是一个群同态，证明 G 一定是阿贝尔群.

*2.109　推广定理 2.128 如下. 设 G 是一个有限(加法)阿贝尔群，阶为 mn，其中 $(m,n)=1$. 定义

$$G_m=\{g\in G: g\text{ 的阶 }\mid m\}\text{ 和 }G_n=\{h\in G: h\text{ 的阶 }\mid n\}.$$

(i)证明 G_m 和 G_n 是满足 $G_m\cap G_n=\{0\}$ 的子群.

(ii)证明 $G=G_m+G_n=\{g+h: g\in G_m\text{ 和 }h\in G_n\}$.

(iii)证明 $G\cong G_m\times G_n$.

*2.110　(i)证明，若整数 m 的素分解是 $m=p_1^{e_1}\cdots p_n^{e_n}$，则

$$\mathbb{I}_m\cong\mathbb{I}_{p_1^{e_1}}\times\cdots\times\mathbb{I}_{p_n^{e_n}},$$

从而推广了定理 2.128.

(ii)证明，若整数 m 的素分解是 $m=p_1^{e_1}\cdots p_n^{e_n}$，则

$$U(\mathbb{I}_m)\cong U(\mathbb{I}_{p_1^{e_1}})\times\cdots\times U(\mathbb{I}_{p_n^{e_n}}),$$

从而推广了推论 2.131.

2.111 (i)设 p 是素数，证明 $\phi(p^k)=p^k\left(1-\frac{1}{p}\right)$.

H (ii)若正整数 h 的所有不同素因子是 p_1，p_2，…，p_n，证明

$$\phi(h)=h\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right).$$

191 H 2.112 设 p 是奇素数，并假设对 $1\leqslant i\leqslant p-1$ 有 $a_i\equiv i \bmod p$. 证明存在一对不同整数 i 和 j 使得 $ia_i\equiv ja_j \bmod p$.

*2.113 若 G 是群，x，$y\in G$，定义它们的**换位子**为 $xyx^{-1}y^{-1}$，定义**换位子子群** G' 为由所有换位子生成的子群(两个换位子的积不一定是换位子).

(i)证明 $G'\lhd G$

(ii)证明 G/G' 是阿贝尔群.

(iii)若 $\varphi: G\to A$ 是一个同态，其中 A 是阿贝尔群，证明 $G'\leqslant\ker\varphi$. 反之，若 $G'\leqslant\ker\varphi$，证明 $\mathrm{im}\varphi$ 是阿贝尔群.

(iv)若 $G'\leqslant H\leqslant G$，证明 $H\lhd G$.

→2.7 群作用

置换群引导我们研究抽象群. 下面这个结果是凯莱(A. Cayley，1821—1895)得到的，它表明抽象群与置换之间的关系并不疏远.

→ **定理 2.132(凯莱)** *每个群 G 是(同构于)对称群 S_G 的一个子群. 特别地，若 G 是阶为 n 的有限群，则 G 是 S_n 的一个子群同构.*

证明 对每个 $a\in G$，定义"平移"$\tau_a: G\to G$，对每个 $x\in G$ 有 $\tau_a(x)=ax$(若 $a\neq 1$，则 τ_a 不是一个同态). 对 a，$b\in G$，$(\tau_a\circ\tau_b)(x)=\tau_a(\tau_b(x))=\tau_a(bx)=a(bx)=(ab)x=\tau_{ab}(x)$，所以

$$\tau_a\tau_b=\tau_{ab}.$$

于是每个 τ_a 是双射，因它的逆是 $\tau_{a^{-1}}$：

$$\tau_a\tau_{a^{-1}}=\tau_{aa^{-1}}=\tau_1=1_G,$$

所以 $\tau_a\in S_G$.

定义 $\varphi: G\to S_G$，$\varphi(a)=\tau_a$，则

$$\varphi(a)\varphi(b)=\tau_a\tau_b=\tau_{ab}=\varphi(ab),$$

所以 φ 是一个同态. 最后，φ 是一个单射. 若 $\varphi(a)=\varphi(b)$，则 $\tau_a=\tau_b$，因此对所有 $x\in G$ 有 $\tau_a(x)=\tau_b(x)$. 特别地，当 $x=1$ 时，得 $a=b$.

后一个命题可由习题 2.65 得到，它是说：若 X 是集合且 $|X|=n$，则 $S_X\cong S_n$. ■

读者可能注意到，在凯莱定理的证明中，置换 τ_a 正是 G 的乘法表中的第 a 行.

说真的，凯莱定理本身只能让人引起一点兴趣，但是，完全一样的证明在更大的环境中却

192 起更大的作用.

→ **定理 2.133(陪集表示定理)** *设 G 是群，H 是 G 的子群且有有限指数 n，则存在一个同态 $\varphi: G\to S_n$ 满足 $\ker\varphi\leqslant H$.*

证明 即使 H 可能不是正规子群，我们在这个证明中仍然记 G 中 H 的所有陪集构成的族为 G/H.

对每个 $a\in G$，定义"平移"$\tau_a: G/H\to G/H$，对每个 $x\in G$ 有 $\tau_a(xH)=axH$. 对 a，$b\in G$，有

$$(\tau_a\circ\tau_b)(xH)=\tau_a(\tau_b(xH))=\tau_a(bxH)=a(bxH)=(ab)xH=\tau_{ab}(aH),$$

因此

$$\tau_a\tau_b=\tau_{ab}.$$

于是每个 τ_a 是双射，因为它的逆是 $\tau_{a^{-1}}$：

$$\tau_a\tau_{a^{-1}}=\tau_{aa^{-1}}=\tau_1=1_{G/H},$$

所以 $\tau_a\in S_{G/H}$. 定义 $\varphi: G\to S_{G/H}$，$\varphi(a)=\tau_a$，则

$$\varphi(a)\varphi(b)=\tau_a\tau_b=\tau_{ab}=\varphi(ab),$$

所以 φ 是一个同态. 最后，若 $a\in\ker\varphi$，则 $\varphi(a)=1_{G/H}$，所以对所有 $x\in G$ 有 $\tau_a(xH)=xH$. 特别地，当 $x=1$ 时，得到 $aH=H$，根据引理 2.82(i)，得 $a\in H$. 结论可由习题 2.65 得到，因为 $|G/H|=n$，所以 $S_{G/H}\cong S_n$. ■

当 $H=\{1\}$ 时，这就是凯莱定理.

我们现在将阶为 1 到 7 的所有群分类. 根据例 2.90，每个阶为素数 p 的群与 $\mathbb{I}_p$ 同构，所以对同构来说，只有一个阶为 p 的群. 在 1 到 7 中，2，3，5，7 这四个数是素数，所以我们只看阶为 4 和 6 的群.

→ **命题 2.134** *每个阶为 4 的群 G 与 $\mathbb{I}_4$ 或 $\mathbf{V}$ 同构. 另外，$\mathbb{I}_4$ 和 $\mathbf{V}$ 不同构.*

证明 根据拉格朗日定理，G 中除了 1 之外每个元素的阶为 2 或 4. 若有一个阶为 4 的元素，则 G 是循环群. 否则，对所有 $x\in G$ 有 $x^2=1$，所以习题 2.44 表明 G 是阿贝尔群.

若选取 G 中不同元素 x 和 y，它们都不是 1，则我们可以很快验证 $xy\notin\{1, x, y\}$，因而

$$G=\{1,x,y,xy\}.$$

容易看出，双射 $f: G\to\mathbf{V}$，$f(1)=1$，$f(x)=(1\ 2)(3\ 4)$，$f(y)=(1\ 3)(2\ 4)$，$f(xy)=(1\ 4)(2\ 3)$，是一个同构，因为在这里，任意两个阶为 2 的元素的积是另一个阶为 2 的元素.

我们在例 2.91 中已经看到 $\mathbb{I}_4\ncong\mathbf{V}$. ■ 193

→ **命题 2.135** *若 G 是阶为 6 的群，则 G 与 $\mathbb{I}_6$ 或 S_3 同构.*[⊖] *另外，$\mathbb{I}_6$ 和 S_3 不同构.*

证明 根据拉格朗日定理，非单位元元素的阶只可能是 2、3 和 6. 当然，若 G 有一个阶为 6 的元素，则 $G\cong\mathbb{I}_6$. 现在习题 2.46 表明 G 一定含有一个阶为 2 的元素，不妨设为 t. 令 $T=\langle t\rangle$.

⊖ 凯莱在 1854 年写的一篇文章中陈述了这个命题. 但是，1878 年他在《美国数学杂志》中写道："一般问题是求出所有阶为 n 的群；…若 $n=6$，则存在三个群；一个是

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5\quad(\alpha^6=1),$$

另两个是

$$1,\ \beta,\ \beta^2,\ \alpha,\ \alpha\beta,\ \alpha\beta^2\quad(\alpha^2=1,\ \beta^3=1),$$

即在第一个群中有 $\alpha\beta=\beta\alpha$，而在另一个群中我们有 $\alpha\beta=\beta^2\alpha$，$\alpha\beta^2=\beta\alpha$."凯莱列出了 $\mathbb{I}_6$，$\mathbb{I}_2\times\mathbb{I}_3$ 和 S_3. 当然，$\mathbb{I}_2\times\mathbb{I}_3\cong\mathbb{I}_6$，甚至荷马也同意这个论述.

因为$[G: T]=3$，所以 T 的陪集上的代表元是一个同态 $\rho: G\to S_{G/T}\cong S_3$，且满足 $\ker\rho\leqslant T$. 因此，$\ker\rho=\{1\}$或 $\ker\rho=T$. 在第一种情形中，ρ 是一个单射，因而它是一个同构，这是因为 $|G|=6=|S_3|$. 在第二种情形中，$\ker\rho=T$，所以 $T\lhd G$ 且商群 G/T 有定义. 在第二种情形中，我们还将看到 G 是循环群. 现在 G/T 是循环群，因为 $|G/T|=3$，所以存在 $a\in G$ 满足$G/T=\{T, aT, a^2T\}$. 另外，ρ_t 是置换

$$\rho_t=\begin{pmatrix} T & aT & a^2T \\ tT & taT & ta^2T \end{pmatrix}.$$

因为 $t\in T=\ker\rho$，所以 ρ_t 是恒等函数. 特别地，根据引理 2.82(i)知，$aT=\rho_t(aT)=taT$，所以 $a^{-1}ta\in T=\{1, t\}$. 但是 $a^{-1}ta\neq1$，所以 $a^{-1}ta=t$，即 $ta=at$. 现在 a 的阶为 3 或 6(因为 $a\neq1$和 $a^2\neq1$). 不管哪种情形，我们都断言 G 有一个阶为 6 的元素. 根据命题 2.129，若 a 的阶为 3，则 at 的阶为 6[只要注意到$(at)^6=1$，且对 $i<6$ 有$(at)^i\neq1$]. 因此，G 是阶为 6 的循环群，且 $G\cong\mathbb{I}_6$.

显然$\mathbb{I}_6$ 和 S_3 不同构，因为一个是阿贝尔群而另一个不是. ■

由这一结果得出$\mathbb{I}_6\cong\mathbb{I}_2\times\mathbb{I}_3$ 的另一个证明(见定理 2.128).

将阶为 8 的群分类是很困难的，因为我们还没有发展出足够的理论. (见作者的另一本书《高等近世代数》[⊖] 中的定理 5.83.)阶为 8 的非同构群仅有 5 个，三个是阿贝尔群，即$\mathbb{I}_8$，$\mathbb{I}_4\times\mathbb{I}_2$ 和$\mathbb{I}_2\times\mathbb{I}_2\times\mathbb{I}_2$；两个是非阿贝尔群，即 D_8 和 **Q**.

我们可以继续讨论更大的阶，但是事情很快会得不到控制，如表 2-4 所示(图中数的计算
194 很复杂). 阶$\leqslant2000$ 的非同构群的数目由欧布莱恩(E. O'Brien)找到. 米科沃(A. McIver)和诺伊曼(P. M. Neumann)证明了，对大数 n，阶为 n 的非同构群的数目大约是 $n^{\mu^2+\mu+2}$，其中 $\mu(n)$是 n 的素分解中的最大指数.

表 2-4

群的阶	群的个数
2	1
4	2
8	5
16	14
32	51
64	267
128	2 328
256	56 092
512	10 494 213
1024	49 487 365 422

群是通过抽象出置换的基本性质而产生的. 但是，置换有一个重要特征在群公理中没有被提到：置换是函数. 我们将看到，当恢复这个特征时会产生一些有趣的结论.

在给出下面这个定义之前，让我们先给出一个记号. 两个变量的函数 $\alpha: X\times Y\to Z$ 可以看作是一个变量的函数构成的单参数族：每个 $x\in X$ 给出一个函数 $\alpha_x: Y\to Z$，即 $\alpha_x(y)=\alpha(x, y)$.

→ **定义** *若 X 是集合，G 是群，称 G 在 X 上作用*[⊜]*，若存在一个函数 $\alpha: G\times X\to X$(称为一个作用)满足*

(i)对 $g, h\in G$ 有 $\alpha_g\circ\alpha_h=\alpha_{gh}$；

⊖ 本书中文版已由机械工业出版社出版. ——编辑注

⊜ 若 G 在 X 上作用，则我们通常称 X 为一个 G-集合.

(ii) $\alpha_1 = 1_X$，即恒等函数.

若 G 在 X 上作用，则我们通常记 $\alpha_g(x)$ 为 gx. 用这个记号时公理(i)为 $g(hx)=(gh)x$.

当然，每个子群 $G \leqslant S_X$ 在 X 上作用. 一般地，群 G 在集合 X 上的作用对应于同态 $G \to S_X$.

→ **命题 2.136** 若 $\alpha: G \times X \to X$ 是群 G 在集合 X 上的一个作用，则 $g \mapsto \alpha_g$ 定义了一个同态 $G \to S_X$. 反之，若 $B: G \to S_X$ 是一个同态，则 $\beta: G \times X \to X$，$\beta(g, x) = B(g)(x)$，是一个作用. 195

证明 若 $\alpha: G \times X \to X$ 是一个作用，则我们断言每个 α_g 是 X 的一个置换. 事实上，其逆为 $\alpha_{g^{-1}}$，因为 $\alpha_g \alpha_{g^{-1}} = \alpha_{gg^{-1}} = \alpha_1 = 1_X$. 于是 $A: G \to S_X$，$A(g) = \alpha_g$，是一个函数. 由公理(i)知 A 是一个同态：

$$A(gh) = \alpha_g h = \alpha_g \circ \alpha_h = A(g) \circ A(h),$$

反之，给定一个同态 $B: G \to S_X$，则函数 $\beta: G \times X \to X$，$\beta(g, x) = B(g)(x)$，是一个作用. 根据我们前面给出的记号，则 $\beta_g = B(g)$. 因此，公理(i)只是说 $B(g) \circ B(h) = B(gh)$，因为 B 是一个同态，所以公理(i)成立. 因为每个同态把单位元映为单位元，所以 $B(1) = 1_X$，公理(ii)成立. ■

凯莱定理是说，群 G 通过(左)平移在自己上作用，该定理的推广形式即陪集表示定理(定理 2.133)表明，G 通过(左)平移也在子群 H 的陪集族上作用.

→ **例 2.137** 我们证明 **G 通过共轭在自己上作用**. 对每个 $g \in G$，定义 $\alpha_g: G \to G$，

$$\alpha_g(x) = gxg^{-1}.$$

为验证公理(i)，注意到对每个 $x \in G$，

$$\begin{aligned}(\alpha_g \circ \alpha_h)(x) &= \alpha_g(\alpha_h(x)) \\ &= \alpha_g(hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= \alpha_{gh}(x).\end{aligned}$$

因此 $\alpha_g \circ \alpha_h = \alpha_{gh}$.

为证明公理(ii)，注意到对每个 $x \in G$，

$$\alpha_1(x) = 1x1^{-1} = x,$$

所以 $\alpha_1 = 1_G$. ◀

以下是两个基本的定义. 196

→ **定义** 若 G 在 X 上作用，且 $x \in X$，则 x 的**轨道**，记为 $\mathcal{O}(x)$，是指 X 的子集：

$$\mathcal{O}(x) = \{gx : g \in G\} \subseteq X;$$

x 的**稳定化子**，记为 G_x，是指 G 的子群：

$$G_x = \{g \in G : gx = x\} \leqslant G.$$

容易验证点 x 的稳定化子 G_x 是 G 的子群.

让我们求出上面例子中的轨道和稳定化子.

例 2.138 (i)凯莱定理是说 G 通过平移 $\tau_a: x \mapsto ax$ 在自己上作用. 若 $x\in G$, 则轨道 $\mathcal{O}(x)=G$, 这是因为若 $g\in G$, 则 $g=(gx^{-1})x$. x 的稳定化子 G_x 是$\{1\}$, 这是因为若 $x=\tau_a(x)=ax$, 则$a=1$. 当存在某个 $x\in X$ 使得$\mathcal{O}(x)=X$ 时, 我们说 G 在 X 上**可迁地作用**.

(ii)当 G 通过平移 $\tau_a: xH \mapsto axH$ 在 G/H(子群 H(不一定正规)的陪集族)上作用时, 轨道$\mathcal{O}(xH)=G/H$, 这是因为若 $g\in G$ 且 $a=gx^{-1}$, 则 $\tau_a: xH\mapsto gH$. 因此 G 在 G/H 上可迁地作用. xH 的稳定化子 G_{xH} 是 xHx^{-1}, 这是因为 $axH=xH$ 当且仅当 $x^{-1}ax\in H$ 当且仅当 $a\in xHx^{-1}$. ◀

例 2.139 设 $X=\{v_0, v_1, v_2, v_3\}$是正方形的顶点集, 并设 G 是在 X 上作用的二面体群 D_8, 如图 2-17所示(为明显起见, 图中的顶点标注为 0, 1, 2, 3, 而不是 v_0, v_1, v_2, v_3).

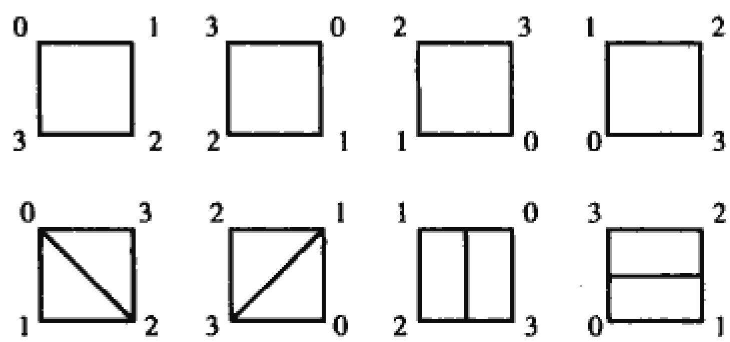


图 2-17 二面体群 D_8

$$G=\{\text{旋转}:(1),(v_0v_1v_2v_3),(v_0v_2)(v_1v_3),(v_0v_3v_2v_1)\}\cup$$

197 $$\{\text{反射}:(v_1v_3),(v_0v_2),(v_0v_1)(v_2v_3),(v_0v_3)(v_1v_2)\}.$$

对每个顶点 $v_i\in X$, 存在 $g\in G$ 使得 $gv_0=v_i$, 因此$\mathcal{O}(v_0)=X$ 且 D_8 可迁地作用.

v_0 的稳定化子 G_{v_0} 是什么? 除了单位元, 只有一个 $g\in D_8$ 固定 v_0, 即 $g=(v_1\ v_3)$, 因此 G_{v_0}是阶为 2 的子群. (这个例子可以被推广到对正 n 边形作用的二面体群 D_{2n}.) ◀

→ **例 2.140** 设 G 通过共轭对自己作用. 若 $x\in G$, 则

$$\mathcal{O}(x)=\{y\in G: y=axa^{-1}, \text{对某个 } a\in G\},$$

此时$\mathcal{O}(x)$称为 x 的**共轭类**, 通常记为 x^G. 例如, 命题 2.33 表明, 若 $\alpha\in S_n$, 则 α 的共轭类由 S_n 中与 α 有相同的循环结构的所有置换构成.

若 $x\in G$, 则 x 的稳定化子 G_x 是

$$C_G(x)=\{g\in G: gxg^{-1}=x\}.$$

G 的这个子群由所有和 x 交换的 $g\in G$ 构成, 称为 G 中 x 的**中心化子**. ◀

例 2.141 设 $X=\{1, 2, \cdots, n\}$, $\sigma\in S_n$, 并把循环群 $G=\langle\sigma\rangle$看作是在 X 上作用. 若 $i\in X$, 则

$$\mathcal{O}(i)=\{\sigma^k(i): k\in \mathbf{Z}\}.$$

设 $\sigma=\beta_1\cdots\beta_{t(\sigma)}$ 是 σ 的完全分解, 并设 $i=i_0$ 被 σ 移动. 若含有 i_0 的循环置换是 $\beta_j=(i_0i_1\cdots i_{r-1})$, 则定理 2.26 的证明表明, 对所有 $k<r-1$ 有 $i_k=\sigma^k(i_0)$. 因此,

$$\mathcal{O}(i)=\{i_0, i_1, \cdots, i_{r-1}\},$$

其中 $i=i_0$. 于是 $|\mathcal{O}(i)|=r$. 若 σ 固定 ℓ，则 ℓ 的稳定化子 G_ℓ 是 G，若 σ 移动 ℓ，则它是 G 的一个真子群. ◀

群 G 在集合 X 上作用可给出 X 上的一个等价关系. 定义

$$x\equiv y \quad \text{当且仅当} \quad \text{存在 } g\in G \text{ 使得 } y=gx.$$

若 $x\in X$，则 $1x=x$，其中 $1\in G$，所以 $x\equiv x$，因而 $\equiv$ 有自反性. 若 $x\equiv y$，则 $y=gx$，则

$$g^{-1}y=g^{-1}(gx)=(g^{-1}g)x=1x=x,$$

所以 $x=g^{-1}y$ 和 $y\equiv x$，因而 $\equiv$ 有对称性. 若 $x\equiv y$ 和 $y\equiv z$，则存在 g，$h\in G$ 满足 $y=gx$ 和 $z=hy$，所以 $z=hy=h(gx)=(hg)x$ 和 $x\equiv z$，因此 $\equiv$ 有传递性，因而它是一个等价关系. $x\in X$ 的等价类是它的轨道，因为

$$[x]=\{y\in X: y\equiv x\}=\{gx: g\in G\}=\mathcal{O}(x).$$ 198

→ **命题 2.142** *若 G 在集合 X 上作用，则 X 是轨道的无交并. 若 X 是有限集，则*

$$|X|=\sum_i |\mathcal{O}(x_i)|,$$

其中 x_i 是从每个轨道中选取的.

证明 由命题 2.20 可得此结论，因为轨道构成 X 的一个分类. 第二个命题给出的计算是正确的：轨道是不相交的，所以 X 中没有元素计算了两次. ■

以下给出了轨道和稳定化子之间的关系.

→ **定理 2.143** *若 G 在集合 X 上作用且 $x\in X$，则*

$$|\mathcal{O}(x)|=[G:G_x]$$

是稳定化子 G_x 在 G 中的指数.

证明 设 G/G_x 即 G 中 G_x 的所有陪集构成的族(我们既没有假设 G_x 是正规子群，也没有假设 G/G_x 是群). 我们将展示一个双射 $\varphi:\mathcal{O}(x)\to G/G_x$，并由此得到结论，因为根据拉格朗日定理的推论 2.84 有 $|G/G_x|=[G:G_x]$. 若 $y\in\mathcal{O}(x)$，则存在 $g\in G$ 有 $y=gx$. 定义 $\varphi(y)=gG_x$. 现在 φ 是定义良好的：若存在 $h\in G$ 使得 $y=hx$，则 $h^{-1}gx=x$，$h^{-1}g\in G_x$，因而 $hG_x=gG_x$. 为看出 φ 是单射，假设 $\varphi(y)=\varphi(z)$，则存在 g，$h\in G$ 满足 $y=gx$，$z=hx$ 和 $gG_x=hG_x$，即 $h^{-1}g\in G_x$. 于是 $h^{-1}gx=x$，所以 $y=gx=hx=z$. 最后，φ 是一个满射：若 $gG_x\in G/G_x$，则设 $y=gx\in\mathcal{O}(x)$，并注意到 $\varphi(y)=gG_x$. ■

在例 2.139 中，D_8 在一个正方形的四个角上作用，我们看到 $|\mathcal{O}(v_0)|=4$，$|G_{v_0}|=2$ 和 $[G:G_{v_0}]=8/2=4$. 在例 2.141 中，$G=\langle\sigma\rangle\leqslant S_n$ 在 $X=\{1,2,\cdots,n\}$ 上作用，我们看到，在 σ 的完全分解 $\sigma=\beta_1\cdots\beta_t(\sigma)$ 中，若 r-循环 β_j 移动 ℓ，则对出现在 β_j 中的任意 ℓ 有 $r=|\mathcal{O}(\ell)|$. 定理 2.143 是说 r 是 σ 的阶为 k 的因子. (但是定理 2.55 告诉我们更多信息：k 是分解中出现的循环置换的长度的最小公倍数.)

→ **推论 2.144** *若有限群 G 在集合 X 上作用，则任意轨道中的元素的个数是 $|G|$ 的因子.*

证明 这可由定理 2.143 和拉格朗日定理立即得出. ■

→ **推论 2.145** *若 x 位于有限群 G 中，则 x 的共轭的个数是其中心化子的指数：*

$$|x^G|=[G:C_G(x)],$$

因而它是 $|G|$ 的因子. 199

证明　和在例 2.140 中一样，x 的轨道是它的共轭类 x^G，而稳定化子 G_x 是中心化子 $C_G(x)$. ■

例 2.29 中的表 2-1 展示了 S_4 中有相同循环结构的置换的个数是 1，6，8，6，3. 注意到每个数都是 $|S_4|=24$ 的因子. 例 2.30 中的表 2-2 展示了 S_5 中相应的数，它们是 1，10，20，30，24，20，15，且所有这些数都是 $|S_5|=120$ 的因子. 我们现在把这些子集当作共轭类，且下面的这个推论解释了为什么这些数整除群的阶.

→　**推论 2.146**　*若 $\alpha\in S_n$，则 S_n 中和 α 有相同循环结构的置换的数目是 $n!$ 的因子.*

证明　只要我们回忆一下命题 2.33，它是说 S_n 中的两个置换在 S_n 中共轭当且仅当它们有相同的循环结构，则由推论 2.145 可立即得出结论. ■

当开始对阶为 6 的群分类时，我们断言任意这样的群有阶为 3 的元素(我们能够利用前面的一个习题断言阶为 2 的元素存在). 我们现在证明每个有限群 G 含有阶为素数 p 的元素，其中 $p \mid |G|$[当 G 是阿贝尔群时，此为命题 2.124(i)].

若群 G 中元素 x 的共轭类 x^G 仅由 x 构成，则 $gxg^{-1}=x$，x 与每个 $g\in G$ 交换，即 $x\in Z(G)$. 反之，若 $x\in Z(G)$，则 $x^G=\{x\}$. 因此，中心 $Z(G)$ 是由 G 中其共轭类只含一个元素的元素构成的.

→　**定理 2.147(柯西)**　*若 G 是一个有限群，其阶可被素数 p 整除，则 G 含有阶为 p 的元素.*

证明　我们对 $|G|$ 应用归纳法来证明这个定理. 基础步骤 $|G|=1$ 显然成立，因为 1 没有素因子. 若 $x\in G$，则 x 的共轭的个数是 $|x^G|=[G:C_G(x)]$，其中 $C_G(x)$ 是 G 中 x 的中心化子. 若 $x\notin Z(G)$，则 x^G 至少有两个元素，所以 $|C_G(x)|<|G|$. 若对某个非中心元素 x 有 $p \mid |C_G(x)|$，则归纳假设是说 $C_G(x)\leqslant G$ 中存在阶为 p 的元素，则我们证明完毕. 因此，我们可以假设对所有非中心元素 $x\in G$ 有 $p\nmid |C_G(x)|$. 由于 $|G|=[G:C_G(x)]|C_G(x)|$，由欧几里得引理得

$$p \mid [G:C_G(x)].$$

回忆 $Z(G)$ 是由所有满足 $|x^G|=1$ 的元素 $x\in G$ 构成的，我们可以利用命题 2.142 看出

200
$$|G|=|Z(G)|+\sum_i [G:C_G(x_i)],$$

其中每个 x_i 是从至少含有两个元素的共轭类中选取的. 由于 $|G|$ 和所有 $[G:C_G(x_i)]$ 被 p 整除，所以 $|Z(G)|$ 被 p 整除. 但是 $Z(G)$ 是阿贝尔群，所以命题 2.124(i) 是说 $Z(G)$ 含有阶为 p 的元素，因而 G 含有阶为 p 的元素. ■

→　**定义**　*有限群 G 的***类方程***是指*

$$|G|=|Z(G)|+\sum_i [G:C_G(x_i)],$$

其中每个 x_i 是从至少含有两个元素的共轭类中选取的.

→　**定义**　*若 p 是素数，则 p-群是指阶为 p^n 的群，其中 $n\geqslant 0$.*

习题 2.117 表明，有限群 G 是 p-群当且仅当 G 中每个元素的阶是 p 的幂.

有些群的中心是平凡的. 例如，$Z(S_3)=\{1\}$. 但是，对于至少含有两个元素的 p-群来说，这是永远不会成立的.

→ **定理 2.148** *若 p 是素数，G 是至少含有两个元素的 p-群，则 $Z(G)\neq\{1\}$.*

证明 我们可假设 G 不是阿贝尔群，因为当 G 是阿贝尔群时定理显然成立. 在类方程 $|G|=|Z(G)|+\sum_i[G:C_G(x_i)]$ 中，每个 $C_G(x_i)$ 是 G 的真子群，这是因为 $x_i\notin Z(G)$. 由于 G 是 p-群，所以 $[G:C_G(x_i)]$ 是 $|G|$ 的因子，因而本身是 p 的幂. 这样，p 整除类方程中除了 $|Z(G)|$ 之外的每一项，所以 $p\mid |Z(G)|$. 因此 $Z(G)\neq\{1\}$. ■

→ **推论 2.149** *若 p 是素数，则每个阶为 p^2 的群 G 是阿贝尔群.*

证明 若 G 不是阿贝尔群，则它的中心 $Z(G)$ 是真子群，根据拉格朗日定理，$|Z(G)|=1$ 或 p. 但是定理 2.148 是说 $Z(G)\neq\{1\}$，所以 $|Z(G)|=p$. 因为中心总是正规子群，所以商群 $G/Z(G)$ 有定义，它的阶为 p，因而 $G/Z(G)$ 是循环群. 这与习题 2.98 矛盾. ■

→ **例 2.150** 对每个素数 p，我们展示一个阶为 p^3 的非阿贝尔群. 定义 $\mathrm{UT}(3,\mathbb{I}_p)$ 为 $\mathrm{GL}(3,\mathbb{I}_p)$ 的子群，它由对角线上全为 1 的上三角形矩阵构成，即 201

$$\mathrm{UT}(3,\mathbb{I}_p)=\left\{\begin{bmatrix}1&a&b\\0&1&c\\0&0&1\end{bmatrix}: a,b,c\in\mathbb{I}_p\right\}.$$

容易看出 $\mathrm{UT}(3,\mathbb{I}_p)$ 是 $\mathrm{GL}(3,\mathbb{I}_p)$ 的子群，其阶为 p^3，这是因为 a，b，c 中每个都有 p 种选择. 读者不难找出 $\mathrm{UT}(3,\mathbb{I}_p)$ 中两个不交换的矩阵. 习题 2.123 是说 $\mathrm{UT}(3,\mathbb{I}_2)\cong D_8$，且命题 6.29 表明，对每个奇素数 p，$A^p=I$ 对所有 $A\in\mathrm{UT}(3,\mathbb{I}_p)$ 成立. ◀

→ **例 2.151** 谁能想到柯西定理和费马定理都是某个普通定理的特殊情形呢?[⊖] 这个定理的证明是由麦克凯(J. H. McKay)给出的. 若 G 是有限群，p 是素数，记 p 个 G 的笛卡尔积为 G^p，并定义

$$X=\{(a_1,a_2,\cdots,a_p)\in G^p: a_1a_2\cdots a_p=1\}.$$

注意 $|X|=|G|^{p-1}$，因为最先的 $p-1$ 个元素是任意选取的，第 p 个元素一定等于 $(a_1a_2\cdots a_{p-1})^{-1}$. 现在通过对 $0\leqslant i\leqslant p-1$ 定义

$$[i](a_1,a_2,\cdots,a_p)=(a_{i+1},a_{i+2},\cdots,a_p,a_1,a_2,\cdots,a_i)$$

把 X 做成一个 $\mathbb{I}_p$-集. 新的 p-元组中元素的积是 $a_1a_2\cdots a_p$ 的一个共轭：

$$a_{i+1}a_{i+2}\cdots a_pa_1a_2\cdots a_i=(a_1a_2\cdots a_i)^{-1}(a_1a_2\cdots a_p)(a_1a_2\cdots a_i).$$

这个共轭是 1(因为 $g^{-1}1g=1$)，所以 $[i](a_1,a_2,\cdots,a_p)\in X$. 根据推论 2.144，$X$ 的每个轨道的长度是 $|\mathbb{I}_p|=p$ 的因子，由于 p 是素数，所以这些长度是 1 或 p. 含有一个元素的轨道是由所有元素 a_i 都相等的 p-元组构成的，这是因为该 p-元组的所有循环置换是相同的. 换句话说，这样的轨道对应于满足 $a^p=1$ 的元素 $a\in G$. 显然，$(1,1,\cdots,1)$ 是这样的轨道. 若它是唯一这样的轨道，则我们会有

$$|G|^{p-1}=|X|=1+kp,$$

其中 $k\geqslant 0$，即 $|G|^{p-1}\equiv 1 \bmod p$. 若 p 是 $|G|$ 的因子，则我们得到一个矛盾，这是因为 $|G|^{p-1}\equiv 0 \bmod p$. 因此我们证明了柯西定理：若素数 p 是 $|G|$ 的因子，则 G 有阶为 p 的元素.

⊖ 若 G 是阶为 n 的群，且 p 是一个素数，则方程 $x^p=1$ 的解 $x\in G$ 的个数模 p 与 n^{p-1} 同余.

现在假设 G 是阶为 n 的群，且 p 不是 n 的因子，例如设 $G=\mathbb{I}_n$. 根据拉格朗日定理，G 没有阶为 p 的元素，所以若 $a\in G$ 和 $a^p=1$，则 $a=1$. 因此，G^p 中长度为 1 的轨道只有 $(1, 1, \cdots, 1)$，所以

$$n^{p-1}=|G|^{p-1}=|X|=1+kp;$$

即，若 p 不是 n 的因子，则 $n^{p-1}\equiv 1 \bmod p$. 两边用 n 相乘得 $n^p\equiv n \bmod p$，这个同余式当 p

202 是 n 的因子时也成立，这就是费马定理. ◀

我们已经在命题 2.99 中看到，A_4 是阶为 12 的群且没有阶为 6 的子群. 因此，断言若 d 是 $|G|$ 的因子则 G 一定有阶为 d 的子群是错误的. 但是，当 G 是 p-群时，这个断言成立. 事实上，不仅如此，G 还一定有阶为 d 的正规子群.

→ **命题 2.152** *若 G 是阶为 $|G|=p^e$ 的群，则对每个 $k\leqslant e$，G 有阶为 p^k 的正规子群.*

证明 我们对 $e\geqslant 0$ 应用归纳法证明这个结论. 基础步骤显然成立，所以只需要看归纳步骤. 根据定理 2.148，G 的中心是非平凡的：$Z(G)\neq\{1\}$. 若 $Z(G)=G$，则 G 是阿贝尔群，且我们已经在命题 2.124 中证明了这个结论. 因此，我们可以假设 $Z(G)$ 是 G 的真子群. 由于 $Z(G)\lhd G$,我们有阶比 $|G|$ 更小的 p-群 $G/Z(G)$. 假设 $|Z(G)|=p^c$. 若 $k\leqslant c$，因为 $Z(G)$ 是阿贝尔群，所以 $Z(G)$ 含有阶为 p^k 的正规子群，因而 G 含有阶为 p^k 的正规子群. 若 $k>c$，则由归纳假设，$G/Z(G)$ 含有阶为 p^{k-c} 的正规子群 S^*. 对应定理给出 G 的一个正规子群 S，它满足

$$Z(G)\leqslant S\leqslant G$$

且 $S/Z(G)\cong S^*$. 根据拉格朗日定理的推论 2.84，

$$|S|=|S^*||Z(G)|=p^{k-c}\cdot p^c=p^k.$$ ■

阿贝尔群(和四元数群)有一个性质：每个子群都是正规的. 其对立面是除了 $\{1\}$ 和 G 之外没有其他正规子群的群.

→ **定义** *群 G 称为单群，若 $G\neq\{1\}$，且除了 $\{1\}$ 和 G 本身外，G 没有其他的正规子群.*

→ **命题 2.153** *阿贝尔群 G 是单群当且仅当它是有限群且阶为素数.*

证明 若 G 是阶为素数 p 的有限群，则除了 $\{1\}$ 和 G 外，G 没有其他的子群 H，否则由拉格朗日定理知 $|H|$ 是 p 的因子. 因此 G 是单群.

反之，假设 G 是单群. 因为 G 是阿贝尔群，所以每个子群是正规的，所以除了 $\{1\}$ 和 G 外，G 没有其他的子群. 选取 $x\in G$ 满足 $x\neq 1$. 由于 $\langle x\rangle$ 是子群，我们有 $\langle x\rangle=G$. 若 x 的阶为无穷，则 x 的所有幂是不同的，所以 $\langle x^2\rangle<\langle x\rangle$ 是 $\langle x\rangle$ 的一个子群，矛盾. 因此，每个 $x\in G$ 的阶有限，不妨设为 m. 若 m 是合数，则 $m=k\ell$，$\langle x^k\rangle$ 是 $\langle x\rangle$ 的非平凡真子群，矛盾. 因此 $G=$

203 $\langle x\rangle$ 的阶为素数. ■

我们现在证明 A_5 是非阿贝尔单群(事实上，它是这样的群中最小的一个. 不存在阶比 60 小的非阿贝尔单群).

假设元素 $x\in G$ 有 k 个共轭，即

$$|x^G|=|\{gxg^{-1}: g\in G\}|=k.$$

若存在子群 $H\leqslant G$ 满足 $x\in H\leqslant G$，则 x 在 H 中有多少个共轭？由于

$$x^H=\{hxh^{-1}: h\in H\}\subseteq\{gxg^{-1}: g\in G\}=x^G,$$

我们有 $|x^H| \leqslant |x^G|$. 可能存在严格的不等式 $|x^H| < |x^G|$. 例如，取 $G=S_3$，$x=(1\ 2)$ 和 $H=\langle x\rangle$. 我们知道 $|x^G|=3$(因为所有的对换都是共轭的)，然而 $|x^H|=1$(因为 H 是阿贝尔群).

现在让我们特别地来考虑一下 $G=S_5$，$x=(1\ 2\ 3)$ 和 $H=A_5$ 这个问题.

引理 2.154 A_5 中所有的 3-循环置换共轭.

证明 设 $G=S_5$，$\alpha=(1\ 2\ 3)$ 和 $H=A_5$. 我们知道 $|\alpha^{S_5}|=20$，这是因为 S_5 中存在 20 个 3-循环置换(正如我们在例 2.30 中所看到的). 因此，根据推论 2.145，$20=|S_5|/|C_{S_5}(\alpha)|=120/|C_{S_5}(\alpha)|$，所以 $|C_{S_5}(\alpha)|=6$，即 S_5 中恰有 6 个置换和 α 交换. 它们是

$$(1),(1\ 2\ 3),(1\ 3\ 2),(4\ 5),(4\ 5)(1\ 2\ 3),(4\ 5)(1\ 3\ 2).$$

最后三个是奇置换，所以 $|C_{A_5}(\alpha)|=3$. 我们得出结论

$$|\alpha^{A_5}|=|A_5|/|C_{A_5}(\alpha)|=60/3=20,$$

即 A_5 中所有的 3-循环置换与 $\alpha=(1\ 2\ 3)$ 共轭. ■

这个引理是说 A_5 是由 3-循环置换生成的，该引理可以从 A_5 推广到所有 A_n 上，$n\geqslant 5$，参看习题 2.127.

引理 2.155 A_5 的每个元素或是 3-循环置换或是一些 3-循环置换的乘积.

证明 若 $\alpha\in A_5$，则 α 是偶数个对换的积：$\alpha=\tau_1\tau_2\cdots\tau_{2n-1}\tau_{2n}$. 因为对换可以由 $\tau_{2i-1}\tau_{2i}$ 聚合，所以只需考虑积 $\tau\tau'$，其中 τ 和 τ' 都是对换. 若 τ 和 τ' 相交，则 $\tau=(i\ j)$，$\tau'=(i\ k)$ 和 $\tau\tau'=(i\ k\ j)$；若 τ 和 τ' 不相交，则 $\tau\tau'=(i\ j)(k\ \ell)=(i\ j)(j\ k)(j\ k)(k\ \ell)=(i\ j\ k)(j\ k\ \ell)$. ■ 204

→ **定理 2.156** A_5 是单群.

证明 我们将证明，若 H 是 A_5 的正规子群，且 $H\neq\{(1)\}$，则 $H=A_5$. 若 H 含有 3-循环置换，则正规性迫使 H 含有其所有的共轭. 根据引理 2.154，H 含有每个 3-循环置换，且根据引理 2.155，$H=A_5$. 因此，只需证明 H 含有 3-循环置换.

因为 $H\neq\{(1)\}$，所以它含有某个 $\sigma\neq(1)$. 我们可以假设 $\sigma=(1\ 2\ 3)$，$\sigma=(1\ 2)(3\ 4)$ 或 $\sigma=(1\ 2\ 3\ 4\ 5)$. 正如我们刚才所说的，若 σ 是 3-循环置换，则证明完毕.

若 $\sigma=(1\ 2)(3\ 4)\in H$，则利用命题 2.32：用 $\beta=(3\ 4\ 5)$ 共轭 σ 得到 $\beta\sigma\beta^{-1}=\sigma'=(1\ 2)(4\ 5)\in H$(因为 $\beta\in A_5$ 和 $H\lhd S_5$). 因而 $\sigma\sigma'=(3\ 4\ 5)\in H$.

若 $\sigma=(1\ 2\ 3\ 4\ 5)\in H$，则利用命题 2.32：用 $\gamma=(1\ 2\ 3)$ 共轭 σ 得到 $\gamma\sigma\gamma^{-1}=\sigma''=(2\ 3\ 1\ 4\ 5)\in H$(因为 $\gamma\in A_5$ 和 $H\lhd S_5$). 因而 $\sigma''\sigma^{-1}=(2\ 3\ 1\ 4\ 5)(5\ 4\ 3\ 2\ 1)=(1\ 2\ 4)\in H$. 我们应该说明最后一个等式是如何产生的. 若 $\sigma\in H$ 且 γ 是 3-循环置换，则 $\gamma\sigma\gamma^{-1}\in H$，所以 $(\gamma\sigma\gamma^{-1})\sigma^{-1}\in H$. 重新组合得 $\gamma(\sigma\gamma^{-1}\sigma^{-1})\in H$. 但是，$\sigma\gamma^{-1}\sigma^{-1}$ 是 3-循环置换，所以 H 含有两个 3-循环置换的积. 我们已经非常小心地选取了 γ 使得两个 3-循环置换的积仍是 3-循环置换.

我们已经证明，在所有的情形中 H 均含有 3-循环置换. 因此，A_5 的正规子群只有 $\{(1)\}$ 和 A_5 本身，所以 A_5 是单群. ■

正如我们将在第 5 章中看到的一样，定理 2.156 成为解释为什么二次公式没有推广到给出 5 次或更高次多项式的根的基本原因.

不用花很多工夫我们就能证明，对每个 $n\geqslant 5$，交错群 A_n 都是单群. 通过观察可知 A_4 不

是单群，这是因为四元群 **V** 是 A_4 的正规子群.

引理 2.157 A_6 是单群.

证明 设 $H\neq\{(1)\}$是 A_6 的正规子群，我们必须证明 $H=A_6$. 假设存在某个 $\alpha\in H$ 满足 $\alpha\neq(1)$并固定某个 i，其中 $1\leqslant i\leqslant 6$. 定义

$$F=\{\sigma\in A_6:\sigma(i)=i\}.$$

注意 $\alpha\in H\cap F$，所以 $H\cap F\neq\{(1)\}$. 由第二同构定理得 $H\cap F\lhd F$. 但是，根据习题 2.130，因为 $F\cong A_5$，所以 F 是单群，因而 F 的正规子群只有$\{(1)\}$和 F. 由于 $H\cap F\neq\{(1)\}$，我们有 $H\cap F=F$，即 $F\leqslant H$. 于是 H 含有 3-循环置换，所以根据习题 2.127，$H=A_6$.

205 我们现在假设不存在 $\alpha\in H$ 满足 $\alpha\neq(1)$并固定某个 i，$1\leqslant i\leqslant 6$. 但是，若我们考虑 A_6 中置换的循环结构，则任意这样的 α 一定有循环结构$(1\ 2)(3\ 4\ 5\ 6)$或$(1\ 2\ 3)(4\ 5\ 6)$. 在第一种情形中，$\alpha^2\in H$ 是一个非平凡置换并固定 1(也固定 2)，矛盾. 在第二种情形中，H 含有 $\alpha(\beta\alpha^{-1}\beta^{-1})$，其中 $\beta=(2\ 3\ 4)$，且容易验证这是 H 的一个非平凡元素并固定 6，矛盾. 因此，这样的正规子群 H 不存在，所以 A_6 是单群. ■

→ **定理 2.158** 对所有 $n\geqslant 5$，A_n 都是单群.

证明 若 H 是 A_n 的非平凡正规子群[即 $H\neq(1)$]，则我们必须证明 $H=A_n$. 根据习题 2.127，只需证明 H 含有 3-循环置换. 若 $\beta\in H$ 是非平凡的，则存在某个 i 被 β 移动，不妨设 $\beta(i)=j\neq i$. 选取 3-循环置换 α 满足固定 i 和移动 j. 置换 α 和 β 不交换：$\beta\alpha(i)=\beta(i)=j$，而 $\alpha\beta(i)=\alpha(j)\neq j$. 于是 $\gamma=(\alpha\beta\alpha^{-1})\beta^{-1}$是 H 的非平凡元素. 但是根据命题 2.32，$\beta\alpha^{-1}\beta^{-1}$是 3-循环置换，所以 $\gamma=\alpha(\beta\alpha^{-1}\beta^{-1})$是两个 3-循环置换的积. 因而 γ 至多移动 6 个符号，不妨设为 i_1，…，i_6. 定义

$$F=\{\sigma\in A_n:\sigma\text{ 固定所有 } i\neq i_1,\cdots,i_6\}.$$

根据习题 2.130，$F\cong A_6$，且 $\gamma\in H\cap F$. 因此 $H\cap F$ 是 F 的非平凡正规子群. 但是 F 是单群，与 A_6 同构，所以 $H\cap F=F$，即 $F\leqslant H$. 因此 H 含有 3-循环置换，所以 $H=A_n$. ■

习题

H 2.114 判断对错并说明理由.

(i)每个群 G 与对称群 S_G 同构.

(ii)阶为 4 的群都是阿贝尔群.

(iii)阶为 6 的群都是阿贝尔群.

(iv)若群 G 在集合 X 上作用，则 X 是群.

(v)若群 G 在集合 X 上作用，且 g，$h\in G$ 满足对某个 $x\in X$ 有 $gx=hx$，则 $g=h$.

(vi)若群 G 在集合 X 上作用，x，$y\in X$，则存在 $g\in G$ 使得 $y=gx$.

(vii)若 $g\in G$，其中 G 是有限群，则 g 的共轭的个数是 $|G|$ 的因子.

(viii)阶为 100 的群都含有阶为 5 的元素.

(ix)阶为 100 的群都含有阶为 4 的元素.

(x)阶为 5^8 的群都包含阶为 5^6 的正规子群.

206 (xi)若 G 是阶为 p^n 的单群，其中 p 是素数，则 $n=1$.

(xii)交错群 A_4 是单群.

(xiii)交错群 A_5 是单群.

(xiv)对称群 S_6 是单群.

2.115　证明每个平移 $\tau_a \in S_G$ 是正则置换(见习题 2.29)，其中 $\tau_a: g \mapsto ag$. 同态 $\varphi: G \to S_G$，$\varphi(a)=\tau_a$ 通常称为 G 的正则表示.

2.116　证明阶为 8 的下述群中没有一对是同构的：

$$\mathbb{I}_8; \mathbb{I}_4 \times \mathbb{I}_2; \mathbb{I}_2 \times \mathbb{I}_2 \times \mathbb{I}_2; D_8; \mathbf{Q}.$$

*H 2.117　若 p 是素数，G 是有限群，其每个元素的阶为 p 的幂，证明 G 是 p-群.

*2.118　证明有限 p-群 G 是单群当且仅当 $|G|=p$.

*2.119　证明 S_4 有与 D_8 同构的子群.

*H 2.120　证明 $S_4/\mathbf{V} \cong S_3$.

2.121　H (i)证明 $A_4 \not\cong D_{12}$.

H (ii)证明 $D_{12} \cong S_3 \times \mathbb{I}_2$.

*2.122　(i)若 H 是 G 的子群，$x \in H$，证明

$$C_H(x) = H \cap C_G(x).$$

H (ii)若 H 是有限群 G 中指数为 2 的子群，$x \in H$，证明 $|x^H| = |x^G|$ 或 $|x^H| = \frac{1}{2}|x^G|$，其中 x^H 是 H 中 x 的共轭类.

*H 2.123　证明例 2.150 中的群 $\mathrm{UT}(3, \mathbb{I}_2)$ 与 D_8 同构.

2.124　H (i)S_5 中有多少个置换和(1 2)(3 4)交换？有多少个偶置换和(1 2)(3 4)交换？

(ii)S_7 中有多少个置换和(1 2)(3 4 5)交换？

(iii)展示 S_7 中和(1 2)(3 4 5)交换的所有置换.

2.125　H (i)证明 A_5 中 5-循环置换的共轭类有两个，每个含有 12 个元素.

(ii)证明 A_5 中的共轭类的长度有 1，12，12，15 和 20.

(iii)证明群 G 的每个正规子群 H 是 G 的共轭类的并，其中有一个是{1}.

(iv)利用(ii)和(iii)给出 A_5 是单群的另一个证明.

*2.126　若 $\sigma, \tau \in S_5$，其中 σ 是 5-循环置换，τ 是对换，证明 $\langle\sigma, \tau\rangle = S_5$.

*2.127　H (i)对所有 $n \geq 3$，证明每个 $\alpha \in A_n$ 是一些 3-循环置换的积.

(ii)证明，若一个正规子群 $H \lhd A_n$ 包含一个 3-循环置换，其中 $n \geq 5$，则 $H = A_n$.（参看引理 2.155 和 2.157.）

2.128　证明 $(A_{10})' = A_{10}$，其中 G' 表示群 G 的换位子子群.（参看习题 2.113.）

H 2.129　证明 S_4 的正规子群只有{(1)}，$\mathbf{V}$，A_4 和 S_4.

*2.130　设 $\{i_1, \cdots, i_r\} \subseteq \{1, 2, \cdots, n\}$，且

$$F = \{\sigma \in A_n : \sigma \text{ 固定所有满足 } i \neq i_1, \cdots, i_r \text{ 的 } i\}.$$

证明 $F \cong A_r$. 207

H 2.131　证明 A_5 是阶为 60 的群，它没有阶为 30 的子群.

2.132　设 $X=\{1, 2, 3, \cdots\}$ 是所有正整数构成的集合，S_X 是 X 上的对称群.

(i)证明 $F_\infty = \{\sigma \in S_X : \sigma \text{ 只移动有限多个 } n \in X\}$ 是 S_X 的子群.

(ii)定义 A_∞ 为 F_∞ 的由 3-循环置换生成的子群. 证明 A_∞ 是一个无限单群.

2.133　H (i)证明，若单群 G 有一个指数为 n 的子群，则 G 与 S_n 的一个子群同构.

H (ii)证明无限单群没有指数为有限数 $n>1$ 的子群.

*H 2.134　设 G 是群，满足 $|G| = mp$，其中 p 是素数，且 $1 < m < p$. 证明 G 不是单群.

注 在比 60 小的所有数中，我们现在证明除 11 之外没有以其他数为阶的非阿贝尔单群(即 12，18，24，30，36，40，45，48，50，54，56)．定理 2.148 排除了所有的素数幂(因为中心总是正规子群)，习题 2.134 排除了所有形如 mp 的数，其中 p 是素数且$m<p$．(我们将在定理 6.25 中完成不存在阶小于 60 的非阿贝尔单群的证明.)

*H 2.135 设 $n\geqslant 3$，证明 A_n 是 S_n 仅有的阶为$\frac{1}{2}n!$ 的子群.

*2.136 证明 A_6 没有素指数的子群.

→2.8 用群计算

我们现在应用群理论做一些精妙的计算.

引理 2.159 (i)设群 G 在集合 X 上作用．若 $x\in X$ 和 $\sigma\in G$，则 $G_{\sigma x}=\sigma G_x\sigma^{-1}$.

(ii)若有限群 G 在有限集 X 上作用，且 x 和 y 位于同一个轨道，则 $|G_y|=|G_x|$.

证明 (i)若 $\tau\in G_x$，则 $\tau x=x$．若 $\sigma x=y$，则有

$$\sigma\tau\sigma^{-1}y=\sigma\tau\sigma^{-1}\sigma x=\sigma\tau x=\sigma x=y.$$

因此，$\sigma\tau\sigma^{-1}$固定 y，所以 $\sigma G_x\sigma^{-1}\leqslant G_y$．反包含可以用同样的方法证明，这是因为 $x=\sigma^{-1}y$.

(ii)若 x 和 y 位于同一个轨道，则存在 $\sigma\in G$ 使得 $y=\sigma x$，所以 $|G_y|=|G_{\sigma x}|=$

208 $|\sigma G_x\sigma^{-1}|=|G_x|$. ■

定理 2.160(伯恩赛德引理)㊀ 设 G 在有限集 X 上作用．若 N 是轨道的个数，则

$$N=\frac{1}{|G|}\sum_{\tau\in G}F(\tau),$$

其中 $F(\tau)$是被 τ 固定的 $x\in X$ 的个数.

证明 列出 X 的元素如下：选取 $x_1\in X$，并列出轨道$\mathcal{O}(x_1)$中的所有元素，不妨设$\mathcal{O}(x_1)=\{x_1,x_2,\cdots,x_r\}$；然后选取 $x_{r+1}\notin\mathcal{O}(x_1)$，并列出$\mathcal{O}(x_{r+1})$中的所有元素 x_{r+1}，x_{r+2}，…；如此继续，直到 X 的所有元素被列出．现在列出 G 的元素 τ_1，τ_2，…，τ_n，并组成下述一个由 0 和 1 构成的阵列，其中

$$f_{i,j}=\begin{cases}1 & \text{若 } \tau_i \text{ 固定 } x_j\\ 0 & \text{若 } \tau_i \text{ 移动 } x_j.\end{cases}$$

	x_1	…	x_r	x_{r+1}	…	x_j	…
τ_1	$f_{1,1}$	…	$f_{1,r}$	$f_{1,r+1}$	…	$f_{1,j}$	…
τ_2	$f_{2,1}$	…	$f_{2,r}$	$f_{2,r+1}$	…	$f_{2,j}$	…
τ_i	$f_{i,1}$	…	$f_{i,r}$	$f_{i,r+1}$	…	$f_{i,j}$	…
τ_n	$f_{n,1}$	…	$f_{n,r}$	$f_{n,r+1}$	…	$f_{n,j}$	…

㊀ 伯恩赛德(Burnside)编写了一本很有影响的书《有限群理论》(The Theory of Groups of Finite Order)，该书出版了两版．在第一版中，他把这个定理归功于弗罗贝尼乌斯(G. Frobenius)．在第二版中，他没有把该定理归功于任何人．然而，这个定理的普遍被接受的名称是伯恩赛德引理．为了避免混淆，诺伊曼(P. M. Neumann)建议把这个定理称做非伯恩赛德引理．伯恩赛德是一位优秀的数学家，有一些定理的确归功于他．例如，伯恩赛德证明了：若 p 和 q 都是素数，则不存在阶为 p^mq^n 的单群.

现在被 τ_i 固定的 x 的个数 $F(\tau_i)$ 是阵列第 i 行中 1 的个数．因此 $\sum_{\tau\in G} F(\tau)$ 是阵列中 1 的个数的总和．我们再来看一下列．第一列中 1 的个数是固定 x_1 的 τ_i 的个数，根据定义，这些 τ_i 构成 G_{x_1}．因此，第 1 列中 1 的个数是 $|G_{x_1}|$．类似地，第 2 列中 1 的个数是 $|G_{x_2}|$．根据引理 2.159(ii)知 $|G_{x_1}|=|G_{x_2}|$．因此根据定理 2.143，标有 $x_i\in\mathcal{O}(x_1)$ 的 r 个列中 1 的个数是

$$r\,|G_{x_1}|=|\mathcal{O}(x_1)|\cdot|G_{x_1}|=(|G|/|G_{x_1}|)\,|G_{x_1}|=|G|.$$ 209

对其他任意轨道也是这样：其列恰含有 $|G|$ 个 1．因此，若有 N 个轨道，则阵列中有 $N|G|$ 个 1．我们得出结论

$$\sum_{\tau\in G}F(\tau)=N\,|G|.$$ ■

我们将利用伯恩赛德引理解决下面一类问题．一面旗上有 6 个(同宽度的)条纹，其中每个条纹可以染成红色、白色或兰色，则这样的带条纹的旗子有多少种？显然，图 2-18 中的两面旗是相同的：上面的旗子翻转过来就是下面的旗子(可以看作是站在旗的前面或后面看旗)．

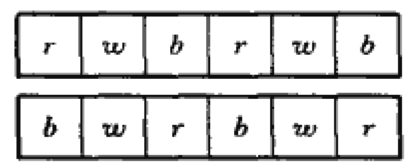


图 2-18　一面旗

设 X 是由这三种颜色组成的所有 6-元组构成的集合．若 $x\in X$，则

$$x=(c_1,c_2,c_3,c_4,c_5,c_6),$$

其中每个 c_i 表示红色、白色或蓝色．设 τ 是翻转所有指标的置换：

$$\tau=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}=(1\ 6)(2\ 5)(3\ 4)$$

(因此，τ“翻转”有色条纹的每个 6-元组 x)．循环群 $G=\langle\tau\rangle$ 在 X 上作用．由于 $|G|=2$，所以任意 6-元组 x 的轨道由 1 个元素或 2 个元素构成：τ 固定 x 或者不固定．由于一面旗子不会因为被翻转而有所改变，所以把一面旗子和一个 6-元组的轨道等同起来是合理的．例如，由 6-元组

$$(r,w,b,r,w,b)\quad 和\quad (b,w,r,b,w,r)$$

构成的轨道描述了图 2-18 中的旗子．因此旗子的数量是轨道的个数 N．根据伯恩赛德引理，有 $N=\frac{1}{2}[F((1))+F(\tau)]$．恒等置换(1)固定每个 $x\in X$，所以 $F((1))=3^6$(有 3 种颜色)．现在 τ 固定 6-元组 x 当且仅当 x 是“回文”(即 x 中的颜色正读反读都一样)．例如，

$$x=(r,r,w,w,r,r)$$

被 τ 固定．反之，若

$$x=(c_1,c_2,c_3,c_4,c_5,c_6)$$ 210

被 $\tau=(1\ 6)(2\ 5)(3\ 4)$ 固定，则 $c_1=c_6$，$c_2=c_5$，$c_3=c_4$，即 x 是一个回文．于是 $F(\tau)=3^3$，这是因为 c_1，c_2 和 c_3 中每一个都有 3 种选择．因此旗子的数量是

$$N=\frac{1}{2}(3^6+3^3)=378.$$

让我们把染色的概念说得更准确些．

定义　给定群 G 在 $X=\{1,\cdots,n\}$ 上的一个作用，$\mathcal{C}$ 是由 q 种颜色构成的集合，则 G 通过

$$\tau(c_1,\cdots,c_n)=(c_{\tau 1},\cdots,c_{\tau n})\quad \tau\in G$$

在集合C^n上作用，其中C^n是由颜色组成的所有n-元组构成的集合．$(c_1, \cdots, c_n)\in C^n$的轨道称为$X$的$(q, G)$-染色．

例 2.161 在一个 4×4 的网格中，把每个小方格染成红色或黑色（相邻的小方格可以染上相同的颜色，事实上，有一种可能是所有的小方格都染成相同的颜色）．

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

13	9	5	1
14	10	6	2
15	11	7	3
16	12	8	4

图 2-19 棋盘

设X是由网格中的 16 个小方格构成的集合，C是由红黑两种颜色构成的集合，则阶为 4 的循环群$G=\langle R\rangle$在X上作用，其中R是 90°的顺时针旋转．图 2-19 可以表明R是怎样作用的：右边的小方格是R对左边小方格的作用结果．在循环记号中，

$$R=(1,4,16,13)(2,8,15,9)(3,12,14,5)(6,7,11,10),$$
$$R^2=(1,16)(4,13)(2,15)(8,9)(3,14)(12,5)(6,11)(7,10),$$
$$R^3=(1,13,16,4)(2,9,15,8)(3,5,14,12)(6,10,11,7).$$

一个红黑棋盘不会因旋转而变化，只是观察它的角度不同罢了．因此，我们可以把棋盘看
211 作是X的$(2, G)$-染色．一个 16-元组的轨道对应着观察棋盘的四个方式．

根据伯恩赛德引理，棋盘的个数是

$$\frac{1}{4}[F((1))+F(R)+F(R^2)+F(R^3)].$$

现在$F((1))=2^{16}$，这是因为每个 16-元组被恒等函数固定．为了计算$F(R)$，注意小方格 1，4，16，13 一定在被R固定的 16-元组中有相同的颜色．类似地，小方格 2，8，15，9 一定有相同的颜色，小方格 3，12，14，5 一定有相同的颜色，小方格 6，7，11，10 一定有相同的颜色．我们得出结论$F(R)=2^4$．注意指数 4 是R的完全分解中循环的个数．类似的分析表明$F(R^2)=2^8$，这是因为R^2的完全分解有 8 个循环．$F(R^3)=2^4$，这是因为R^3的循环结构与R的循环结构相同．因此棋盘的个数是

$$N=\frac{1}{4}[2^{16}+2^4+2^8+2^4]=16\,456.$$

不用群论做这种计算是很困难的，因为很可能会把相同的棋盘至少计算了两次． ◀

我们现在证明一个置换τ的循环结构允许我们计算$F(\tau)$．

引理 2.162 设C是由q种颜色构成的集合，并设$\tau\in S_n$．

(i)若$F(\tau)$是被τ固定的$x\in C^n$的个数，$t(\tau)$是τ的完全分解中循环置换的个数，则

$$F(\tau)=q^{t(\tau)}.$$

(ii)若有限群G在$X=\{1, \cdots, n\}$上作用，则X的(q, G)-染色的个数是

$$N=\frac{1}{|G|}\sum_{\tau\in G}q^{t(\tau)},$$

其中$t(\tau)$是τ的完全分解中循环置换的个数．

证明 (i)设$\tau\in S_n$且$\tau=\beta_1\cdots\beta_t$是一个完全分解，其中每个$\beta_j$是$r_j$循环置换．若$i_1, \cdots, i_{r_j}$是被$\beta_j$移动的符号，则对$k<r_j$有$i_{k+1}=\tau^k i_1$．因为$\tau$固定$x=(c_1, \cdots, c_n)$，所以$\tau(c_1, \cdots, c_n)=$

$(c_{\tau 1}, \cdots, c_{\tau n})=(c_1, \cdots, c_n)$. 因此 $c_{\tau i_1}=c_{i_1}$，所以 $c_{\tau i_1}$ 和 c_{i_1} 有相同的颜色．但是 $\tau^2 i_1$ 也和 i_1 有相同的颜色．实际上，对所有 k，$\tau^k i_1$ 和 i_1 都有相同的颜色．现在可以用另一种方式来看待这些坐标．根据例 2.141，坐标 $\tau^k i_1$ 恰是被 β_j 移动的符号，即 $\beta_j=(i_1, i_2, \cdots, i_{r_j})$．因此，对每个 j，若 $(c_1, \cdots, c_n)$ 被 τ 固定，则被 β_j 移动的所有符号 c_k 一定有相同的颜色．因为存在 q 种颜色和 $t(\tau)$ 个 β_j，所以有 $q^{t(\tau)}$ 个 n-元组被 τ 固定．

(ii) 在伯恩赛德引理中用 $q^{t(\tau)}$ 代替公式中的 $F(\tau)$ 即可得．■ 212

例 2.163　我们现在可以简化例 2.161 中的计算．设 X 是 4 个元素 1，R，R^2，R^3 组成的所有 4×4 网格构成的集合，群 G 在 X 上作用．这些元素的完全分解已在例 2.161 中给出，由此可以看出

$$t((1))=16,\quad t(R)=4=t(R^3),\quad t(R^2)=8.$$

由定理 2.162 得

$$N=\frac{1}{4}[2^{16}+2\cdot 2^4+2^8].$$ ◀

我们引入多变量的多项式，以便陈述由波利亚得到的一个更精美的计数结果．

定义　若 $\tau\in S_n$ 的完全分解有 $e_r(\tau)\geqslant 0$ 个 r-循环置换，则 τ 的**指数**是指单项式

$$\operatorname{ind}(\tau)=x_1^{e_1(\tau)}x_2^{e_2(\tau)}\cdots x_n^{e_n(\tau)}.$$

若 G 是 S_n 的子群，则 G 的**循环指数**是指系数在$\mathbb{Q}$中的有 n 个变量的多项式：

$$P_G(x_1,\cdots,x_n)=\frac{1}{|G|}\sum_{\tau\in G}\operatorname{ind}(\tau).$$

在前面关于带有条纹的旗子的讨论中，群 G 是阶为 2 的循环群，其生成元为 $\tau=(1\ 6)(2\ 5)(3\ 4)$．因此，$\operatorname{ind}((1))=x_1^6$，$\operatorname{ind}(\tau)=x_2^3$，以及

$$P_G(x_1,\cdots,x_6)=\frac{1}{2}(x_1^6+x_2^3).$$

作为另一个例子，考虑有 9 个条纹的所有蓝白旗．这里 $|X|=9$，$G=\langle\tau\rangle\leqslant S_9$，其中

$$\tau=(1\ 9)(2\ 8)(3\ 7)(4\ 6)(5).$$

现在，$\operatorname{ind}((1))=x_1^9$，$\operatorname{ind}(\tau)=x_1x_2^4$，因此 $G=\langle\tau\rangle$ 的循环指数是

$$P_G(x_1,\cdots,x_9)=\frac{1}{2}(x_1^9+x_1x_2^4).$$

在例 2.161 中，我们看到阶为 4 的循环群 $G=\langle R\rangle$ 在一个有 16 个小方格的网格上作用，且

$$\operatorname{ind}((1))=x_1^{16};\quad \operatorname{ind}(R)=x_4^4;\quad \operatorname{ind}(R^2)=x_2^8;\quad \operatorname{ind}(R^3)=x_4^4.$$

因此循环指数是

$$P_G(x_1,\cdots,x_{16})=\frac{1}{4}(x_1^{16}+x_2^8+2x_4^4).$$ 213

命题 2.164　若 $|X|=n$，G 是 S_n 的子群，则 X 的 (q, G)-染色的个数是 $P_G(q, \cdots, q)$，其中 $P_G(x_1, \cdots, x_n)$ 是循环指数．

证明　根据命题 2.162，X 的 (q, G)-染色的个数是

$$\frac{1}{|G|}\sum_{\tau\in G}q^{t(\tau)},$$

其中 $t(\tau)$ 是 τ 的完全分解中循环置换的个数. 另一方面,

$$P_G(x_1,\cdots,x_n)=\frac{1}{|G|}\sum_{\tau\in G}\operatorname{ind}(\tau)$$
$$=\frac{1}{|G|}\sum_{\tau\in G}x_1^{e_1(\tau)}x_2^{e_2(\tau)}\cdots x_n^{e_n(\tau)}.$$

所以

$$P_G(q,\cdots,q)=\frac{1}{|G|}\sum_{\tau\in G}q^{e_1(\tau)+e_2(\tau)+\cdots+e_n(\tau)}$$
$$=\frac{1}{|G|}\sum_{\tau\in G}q^{t(\tau)}.$$ ■

让我们再次计算例 2.161 中有 16 个小方格的红黑棋盘的个数. 这里,

$$P_G(x_1,\cdots,x_{16})=\frac{1}{4}(x_1^{16}+x_2^8+2x_4^4).$$

所以棋盘的个数是

$$P_G(2,\cdots,2)=\frac{1}{4}(2^{16}+2^8+2\cdot 2^4).$$

我们引入循环指数的概念是为了陈述波利亚(Pólya)定理. 一面旗子有 9 个条纹, 其中 4 个蓝色条纹和 5 个白色条纹, 这样的蓝白旗子有多少种? 一般地, 我们想计算轨道的个数, 由此描述任意给定颜色的"条纹"的个数.

定理 2.165(波利亚) 设 $G\leqslant S_X$, 其中 $|X|=n$, 设 $|C|=q$, 且对每个 $i\geqslant 1$ 定义 $\sigma_i=c_1^i+\cdots+c_q^i$. 对每个 r, 若 X 中有 f_r 个元素含有颜色 c_r, 则 X 的 (q, G)-染色的个数是 $P_G(\sigma_1, \cdots,$
214 $\sigma_n)$ 中 $c_1^{f_1}c_2^{f_2}\cdots c_q^{f_q}$ 的系数.

波利亚定理的证明可以在有关组合的书中找到[例如, 看毕格斯(Biggs)的《离散数学》(Discrete Mathematics)或塔克(Tucker)的《应用组合数学》(Applied Combinatorics)]. 为解决上面提出的旗子问题, 首先注意到有 9 个条纹的蓝-白旗子的循环指数是

$$P_G(x_1,\cdots,x_9)=\frac{1}{2}(x_1^9+x_1x_2^4).$$

所以旗子的个数是 $P_G(2, \cdots, 2)=\frac{1}{2}(2^9+2^5)=272$. 利用波利亚定理, 有 4 个蓝色条纹和 5 个白色条纹的旗子的个数是

$$P_G(\sigma_1,\cdots,\sigma_9)=\frac{1}{2}[(b+w)^9+(b+w)(b^2+w^2)^4]$$

中 b^4w^5 的系数. 用二项式定理可算出 b^4w^5 的系数是 66.

习题

H 2.137 判断对错并说明理由.

(i)若有限群 G 在集合 X 上作用, 则 X 一定是有限集.

(ii)若群 G 在有限集 X 上作用, 则 G 一定是有限群.

(iii)若群 G 在集合 X 上作用, x, $y\in X$, 则 $G_x\cong G_y$.

(iv)若群 G 在集合 X 上作用, 且 x, $y\in X$ 位于相同的轨道, 则 $G_x\cong G_y$.

(v)若 D_{10} 在有 5 颗珠子的手镯上作用，则 $\tau\in D_{10}$ 的循环结构是(1)，(1 2)(3 4)或(1 2 3 4 5).

(vi)若 D_{10} 在有 5 颗珠子的手镯上作用，τ 是关于穿过一个珠子且垂直于正面的轴的反射，则 τ 的循环指数是 $x_1x_2^2$.

H 2.138 一面旗子有 n 个条纹，每个条纹用 q 种颜色染色，则这样的旗子有多少种？

2.139 设 X 是 $n\times n$ 网格中的所有小方格，ρ 是 90°的旋转. 定义一个棋盘为一个 (q, G)-染色，其中阶为 4 的循环群 $G=\langle\rho\rangle$ 在作用. 证明棋盘的个数是

$$\frac{1}{4}\left(q^{n^2}+q^{\lfloor(n^2+1)/2\rfloor}+2q^{\lfloor(n^2+3)/4\rfloor}\right),$$

其中 $\lfloor x\rfloor$ 是不大于 x 的最大整数.

2.140 设 X 是一个分解为 n 个扇形的圆盘，ρ 是 $(360/n)^\circ$ 的旋转. 定义一个赌盘为一个 (q, G)-染色，其中阶为 n 的循环群 $G=\langle\rho\rangle$ 在作用. 证明，若 $n=6$，则存在 $\frac{1}{6}(2q+2q^2+q^3+q^6)$ 个含 6 个扇形的赌盘.

[计算含 n 个扇形的赌盘个数的公式是

$$\frac{1}{n}\sum_{d\mid n}\phi(n/d)q^d,$$

其中 ϕ 是欧拉 ϕ-函数.] 215

2.141 设 X 是一个正 n 边形的顶点集合，设二面体群 $G=D_{2n}$ 作用(如通常的对称群一样[见例 2.64]). 定义一个手镯为一个正 n 边形的 (q, G)-染色，并称它的每个顶点为一个珠子. (我们不仅可以旋转一个手镯，还可以掷它.)

H (i)有 5 个珠子的手镯有多少，其中每个珠子可以用 q 种颜色染色？

H (ii)有 6 个珠子的手镯有多少，其中每个珠子可以用 q 种颜色染色？

H (iii)有 6 个珠子的手镯有多少，其中有 1 个红色珠子，2 个白色珠子和 3 个蓝色珠子？ 216

第3章 交换环 I

→3.1 基本性质

在中学代数中，实数的普通加法和乘法通常被赋予一列“法则”，这些法则[⊖]总是很多，也许有 20 个或者更多. 例如，其中之一是**加法消去律**：

$$若\ a+c=b+c,\quad 则\ a=b$$

有些法则也和这个法则一样，仅涉及减法的性质：等式两边减去 c. 但有些法则涉及两种运算，其中一个是**分配律**：

$$(a+b)c=ac+bc;$$

从左读到右，是说 c 可以被“乘进”$a+b$ 中去；从右读到左，是说 c 可以从 $ac+bc$ 中“提取出来”. 还有一个“神秘的”法则：

$$(-1)\times(-1)=1. \tag{M}$$

我们可以删去一些法则，这样做除了法则少可以产生明显节俭的原因外，还有一个很好的理由：较少的法则可以让我们更容易看出数和其他对象之间的相似点，例如多项式、同余类也可以相加相乘. 在探究这些相似点之前，我们先解开(M)的神秘之处.

217 **引理 3.1** 对每个数 a 有 $0\cdot a=0$.

证明 由于 $0=0+0$，所以由分配律得

$$0\cdot a=(0+0)\cdot a=(0\cdot a)+(0\cdot a).$$

等式两边减去 $0\cdot a$(即，使用加法消去律)得 $0\cdot a=0$. ■

我们现在来看为什么不能用 0 去除一个数：给定数 b，它的倒数 $1/b$ 必须满足 $b(1/b)=1$. 特别地，$1/0$ 将是满足 $0\cdot(1/0)=1$ 的数. 但由引理 3.1 知 $0\cdot(1/0)=0$，与 $1\neq 0$ 矛盾.

引理 3.2 若 $(-a)+a=0$，则 $(-1)(-a)=a$.

证明 由分配律和引理 3.1 得

$$0=0\cdot(-a)=(-1+1)(-a)=(-1)(-a)+(-a);$$

两边加上 a 得 $a=(-1)(-a)$. ■

令 $a=1$ 就知道(M)的神秘之处了.

在证明一些初等性质时，让我们先证明积 $(-1)a$ 与 $-a$ 是相同的.

推论 3.3 对每个数 a 有 $(-1)a=-a$.

证明 由引理 3.2，$(-1)(-a)=a$. 两边乘以 -1 得

$$(-1)(-1)(-a)=(-1)a.$$

但是由引理 3.2 知 $(-1)(-1)=1$，所以 $-a=(-1)a$. ■

⊖ 参见 1923 年 Macmillan 出版的霍尔(H. S. Hall)和奈特(S. R. Knight)编著的《大学代数》(Algebra for Colleges and Schools)，或 1937 年 Sanborn 出版的斯通(J. C. Stone)和玛丽(V. S. Mallory)编著的《高等代数》(A Second Course in Algebra).

除了数之外，其他数学对象也可以被加、被乘．例如，在微积分中我们可以对函数进行加乘运算．常数函数 $\varepsilon(x)\equiv 1$ 在乘法中的作用就象数 1 一样，即 $\varepsilon f=f$．引理 3.2 的类似结论 $[-\varepsilon(x)][-f(x)]=f(x)$ 成立吗？回答是肯定的，且结论的证明与对数的证明是完全一样的：只要用 $f(x)$ 代替 a，用 ε 代替 1 即可．

我们现在着重考虑普通加法和普通乘法所拥有的简单性质，并将它们提高到公理的地位．本质上，我们正在描述更多的一般对象，它们都是我们将要研究的．

→ **定义** **交换环**[⊖] R 是指带有两个叫做加法和乘法运算的集合，满足： 218

(i)对所有 a，$b\in R$ 有 $a+b=b+a$；

(ii)对所有 a，b，$c\in R$ 有 $a+(b+c)=(a+b)+c$；

(iii)存在 $0\in R$ 使对所有 $a\in R$ 有 $0+a=a$；

(iv)对任意 $a\in R$，存在 $a'\in R$ 使 $a'+a=0$；

(v)对所有 a，$b\in R$ 有 $ab=ba$；

(vi)对所有 a，b，$c\in R$ 有 $a(bc)=(ab)c$；

(vii)存在 $1\in R$，叫做**单位元**[⊜]，满足对每个 $a\in R$ 有 $1a=a$；

(viii)对所有 a，b，$c\in R$ 有 $a(b+c)=ab+ac$．

当然，公理(i)到(iv)是说 R 在加法下是一个阿贝尔群．因为交换环 R 中加法和乘法是两个运算，所以存在函数

$$\alpha: R\times R\to R \quad \text{满足}\ \alpha(r,r')=r+r'\in R$$

和

$$\mu: R\times R\to R \quad \text{满足}\ \mu(r,r')=rr'\in R,$$

其中任意 r，$r'\in R$．因为 α，μ 是单值函数，所以替换律是成立的：若 $r=r'$，$s=s'$，则 $r+s=r'+s'$，$rs=r's'$．例如，引理 3.1 的证明以 $\mu(0,a)=\mu(0+0,a)$ 开始，引理 3.2 的证明以 $\alpha(0,-a)=\alpha(-1+1,-a)$ 开始．

例 3.4 (i)读者可以设想 $\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$ 带上普通加法和乘法作成交换环(环的公理在数学的建立过程中已经被验证过)．

(ii)设 $\mathbb{Z}[i]$ 是所有形如 $a+bi$ 的复数构成的集合，其中 a，$b\in\mathbb{Z}$，$i^2=-1$．实际上，检验 $\mathbb{Z}[i]$ 是交换环是一个烦人的练习(在引入子环的概念之后，这个练习可以大大地缩简)．$\mathbb{Z}[i]$ 称为**高斯整数环**． 219

(iii)考虑由形如

$$x=a+b\omega$$

的所有实数构成的集合 R，其中 a，$b\in\mathbb{Q}$，$\omega=\sqrt[3]{2}$．易见 R 在普通加法下是封闭的．但是，若 R 在乘法下是封闭的，则 $\omega^2\in R$，且存在有理数 a，b 使得

⊖ 这个术语可能是 1897 年希尔伯特(D. Hilbert)在写 Zahlring 时碰巧想到的．“环(ring)”在德语中的含义之一和在英语中的含义一样，都是“集中”的意思，与在“a ring of theives (一群贼)”中的含义相同．(也有人认为，希尔伯特使用这个术语是因为对一群代数整数来说，每个元素的一个适当的幂可以“循环回到”低次幂的一个线性组合．)

⊜ 有些作者不要求交换环含有 1．对他们来说，所有偶整数构成的集合是一个交换环，但我们不这样认为．他们把我们的环看作含 1 的交换环．

$$\omega^2 = a + b\omega.$$

两边乘以 ω 得：

$$\begin{aligned} 2 &= a\omega + b\omega^2 \\ &= a\omega + b(a + b\omega) \\ &= a\omega + ab + b^2\omega \\ &= ab + (a + b^2)\omega. \end{aligned}$$

若 $a+b^2=0$，则 $a=-b^2$，最后一个式子给出 $2=ab$，因而 $2=(-b^2)b=-b^3$. 但这说明 2 的立方根是有理数，与习题 1.54(ii)矛盾. 因此，$a+b^2\neq 0$，$\omega=(2-ab)/(a+b^2)$. 由于 a，b 都是有理数，所以 ω 是有理数，又与习题 1.54(ii)矛盾. 因此 R 在乘法下不封闭，所以 R 不是交换环. ◀

→ **注** 存在一些非交换环的例子，即带有加法和乘法的集合，满足交换环定义中除公理 $ab=ba$ 外的其他公理. [实际上，在非交换环的定义中用公理 $1a=a=a1$ 代替了公理 $1a=a$，且用两个分配律代替了分配律，即右分配律 $a(b+c)=ab+ac$ 和左分配律 $(b+c)a=ba+ca$.] 例如，设 M 表示所有 2×2 矩阵构成的集合. 例 2.48(i)定义了矩阵的乘法，现在定义加法为

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}.$$

易见 M 带上这个加法以及乘法运算满足非交换环的所有公理，但 M 不是交换环.

220 尽管有许多让人感兴趣的非交换环的例子，但我们在本书中将只讨论交换环.

命题 3.5 引理 3.1 和 3.2 以及推论 3.3 对每个交换环都成立.

证明 这三个结论都可以只利用交换环的定义来证明. 为说明这一点，我们现在证明引理 3.1：若 R 是一个交换环，$a\in R$，则 $0\cdot a=0$.

因为 $0=0+0$，所以由分配律知

$$0\cdot a = (0+0)\cdot a = (0\cdot a) + (0\cdot a).$$

两边加上 $-(0\cdot a)$ 得

$$-(0\cdot a) + (0\cdot a) = -(0\cdot a) + [(0\cdot a) + (0\cdot a)].$$

由 $-(0\cdot a)$ 的定义知等式左边为 $-(0\cdot a)+(0\cdot a)=0$，因此

$$0 = -(0\cdot a) + [(0\cdot a) + (0\cdot a)].$$

我们使用结合律来简化右边

$$\begin{aligned} 0 &= -(0\cdot a) + [(0\cdot a) + (0\cdot a)] \\ &= [-(0\cdot a) + (0\cdot a)] + (0\cdot a) \\ &= 0 + (0\cdot a) \\ &= 0\cdot a. \end{aligned}$$

■

这样详细的证明并不多见，因为它可能使简单的问题复杂化. 你应该把证明看成是对命题成立的原因的解释. 但这个解释对于不同的对象是不同的：一个是给刚开始上高中的学生，一个是给你的同学，还有一个是给你的教授. 根据经验，你的证明应该描述给和你水平相当的

人，其中包括你自己. 让你的证明尽量清晰，不能太长，也不要太短. 如果你的证明受到了质疑，那你必须准备对它进行进一步的解释. 所以，你应该尝试通过对你最初的证明给出足够的细节来预见到存在的质疑.

像$(-1)(-a)=a$这样的公式能够成立，不是因为数a和1的本性，也不是因为加法和乘法运算有什么特殊的定义，而仅仅是因为交换环定义中给出的关于加法和乘法的公理. 例如，我们将在命题3.6中看到：在任意交换环中二项式定理成立. 一旦我们知道了所有函数$\mathbb{R}\to\mathbb{R}$构成一个交换环[见例3.10]，就可以得出二项式定理$(f+g)^n=\sum\binom{n}{i}f^ig^{n-i}$对所有函数$f, g:\mathbb{R}\to\mathbb{R}$都成立的结论. 因此，关于交换环的定理不仅可以应用于数还可以应用于其他领域，从而一下子证明了许多定理，而不是一个个地证明. 这种抽象法使我们的工作效率更高些，相同的结果不必一次又一次地证明. 抽象法还有一个优点. 虽然我们用来加和乘的事物可 221
能非常复杂，但是它们的许多性质可能是由操纵它们的法则得到的，而不是由它们的内部结构得到的. 因此，正如我们在学习群时所看到的一样，抽象法使得我们能聚焦于一个问题的本质部分，而不必把与一个特殊问题无关的特征加以抽象.

→ **定义** 若R是交换环，且$a, b\in R$，则定义**减法**为

$$a-b=a+(-b).$$

根据推论3.3，

$$a-b=a+(-1)b.$$

这里有一个极其繁琐的证明(我们再也不会这么繁琐了!)：分配律$ca-cb=c(a-b)$对减法也成立.

$$\begin{aligned}a(b-c)&=a[b+(-1)c]=ab+a[(-1)c]\\&=ab+[a(-1)]c=ab+[(-1)a]c\\&=ab+(-1)(ac)=ab-ac.\end{aligned}$$

设R是一个交换环，$r\in R$，自然地把rr记为r^2，把rrr记为r^3. 类似的，很自然地把$r+r$记为$2r$，把$r+r+r$记为$3r$. 下面给出正式的定义.

→ **定义** 设R是一个交换环，$a\in R$，$n\in\mathbb{N}$，定义$0a=0$(左边的0是数0，而右边的0是R的零元素)，并定义$(n+1)a=na+a$，定义$(-n)a=-(na)$.

这样，若$a\in R$，$n\in\mathbb{N}$，则$na=a+a+\cdots+a$，其中n是被加数. 易知$(-n)a=-(na)=n(-a)$. R的元素$n^*=n1=1+\cdots+1$(1是R的单位元)具有这样的性质：n^*a等于刚才定义的na. 因此，一个自然数与环中元素的乘积na可以看作是环中两个元素的乘积.

命题3.6(二项式定理) 设R是一个交换环，$a, b\in R$，则对所有$n\geqslant 0$有

$$(a+b)^n=\sum_{r=0}^{n}\binom{n}{r}a^rb^{n-r}.$$

证明 改写关于整数的二项式定理(命题1.18)的证明即可. 特别地，对每个$a\in R$，甚至$a=0$，定义$a^0=1$. ∎

交换环的定义不要求$1\neq 0$. 222

命题 3.7 若 R 是一个交换环且 $1=0$，则 R 仅含有一个元素：$R=\{0\}$. 我们称 R 为**零环**.

证明 若 $r\in R$，则由命题 3.5 知 $r=1r=0r=0$. ■

零环偶而出现，但是我们对它不感兴趣.

定义 交换环 R 称为**整环**，若 $1\neq 0$ 且**乘法消去律**成立：当 $ca=cb$，$c\neq 0$ 时 $a=b$.

我们熟悉的交换环$\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$都是整环，等下我们将给出几个不是整环的交换环的例子.

命题 3.8 非零交换环 R 是整环当且仅当 R 的任意两个非零元素的乘积是非零的.

证明 假设 R 是整环，则乘法消去律成立. 用反证法，假设存在非零元素 a，$b\in R$ 使 $ab=0$. 由命题 3.5 得 $0\cdot b=0$，所以 $ab=0\cdot b$. 由消去律得 $a=0$（因为 $b\neq 0$），矛盾.

反之，假设 R 的任意两个非零元素的乘积是非零的. 若 $ca=cb$ 且 $c\neq 0$，则 $0=ca-cb=c(a-b)$. 由于 $c\neq 0$，由假设非零元素的积不为零知 $a-b=0$. 因此 $a=b$，这正是我们要证明的. ■

一般来说，环 R 的子环是一个子集，且是一个其加法和乘法运算与 R 中的一样的环.

定义 交换环 R 的一个子集 S 称为 R 的**子环**，若

(i) $1\in S$；⊖

(ii) 若 a，$b\in S$，则 $a-b\in S$；

(iii) 若 a，$b\in S$，则 $ab\in S$.

223 和子群是群一样，交换环的子环也是交换环.

命题 3.9 交换环 R 的子环 S 本身也是交换环.

证明 由假设知 $1\in S$. 因为对所有 $r\in R$ 有 $1r=r$，特别地，对所有 $s\in S$ 有 $1s=s$. 我们现在证明 S 在加法下是封闭的：若 s，$s'\in S$，则 $s+s'\in S$. 根据子环定义中的公理(ii)知 $0=1-1\in S$，该公理还表明当 $b\in S$ 时 $0-b=-b\in S$. 最后，若 a，$b\in S$，则由引理 3.3 知

$$a-(-b)=a+(-1)(-b)=a+(-1)(-1)b=a+b.$$

因此，S 在加法和乘法下是封闭的. S 包含 1 和 0，且对任意 $s\in S$ 有 $-s\in S$. S 还继承了交换环定义中的其他公理. 例如，我们知道分配律 $a(b+c)=ab+ac$ 对所有 a，b，$c\in R$ 都成立. 特别地，该等式对所有 a，b，$c\in S\subseteq R$ 也成立，因此分配律在 S 中亦成立. ■

要证明集合 S 是一个交换环需要验证 10 条：在加法和乘法下的封闭性以及其他 8 个公理. 要证明一个交换环的子集 S 是子环只需要验证 3 条，这明显更简单些. 例如，证明高斯整数环

$$\mathbb{Z}[i]=\{z\in\mathbb{C}: z=a+ib: a,b\in\mathbb{Z}\}$$

是$\mathbb{C}$的一个子环，比验证交换环定义中的所有公理都简单. 当然我们首先要证明$\mathbb{C}$是一个交换环.

例 3.10 若 $n\geqslant 3$ 是整数，则令 $\zeta_n=e^{2\pi i/n}$ 是 n 次本原单位根，定义

$$\mathbb{Z}[\zeta_n]=\{z\in\mathbb{C}: z=a_0+a_1\zeta_n+a_2\zeta_n{}^2+\cdots+a_{n-1}\zeta_n^{n-1}, \text{所有 } a_i\in\mathbb{Z}\}.$$

当 $n=4$ 时，$\mathbb{Z}[\zeta_4]$是高斯整数$\mathbb{Z}[i]$. 易验证$\mathbb{Z}[\zeta_n]$是$\mathbb{C}$的一个子环. 为证明$\mathbb{Z}[\zeta_n]$在乘法下封闭，要注意到：若 $m\geqslant n$，则 $m=qn+r$，其中 $0\leqslant r<n$，且 $\zeta_n^m=\zeta_n^r$. ◀

⊖ 偶整数不能构成$\mathbb{Z}$的子环，因为 1 不是偶数. 在介绍了理想的概念之后，我们将会认识它们的特殊结构.

以下是交换环不为整环的例子.

→ **例 3.11** (i)设$\mathcal{F}(\mathbb{R})$是所有函数$\mathbb{R}\to\mathbb{R}$构成的集合，带有**点态加法**和**点态乘法**两种运算：对函数 $f, g\in\mathcal{F}(\mathbb{R})$，定义函数 $f+g$ 和 fg 为

$$f+g: a\mapsto f(a)+g(a) \text{ 和 } fg: a\mapsto f(a)g(a)$$

(注意 fg 不是它们的合成). 224

准确地说点态加法和点态乘法运算是微积分中出现的函数上的运算. 例如，回忆导数的乘法法则：

$$(fg)' = f'g + fg'.$$

$f'g+fg'$中的"+"是点态加法运算，fg 是 f 和 g 点态乘法运算.

我们断言，带着这些运算的$\mathcal{F}(\mathbb{R})$是一个交换环. 公理的验证留给读者，我们只给出提示：$\mathcal{F}(\mathbb{R})$中的零元素是取值为 0 的常数函数 z[即，对所有 $a\in\mathbb{R}$ 有 $z(a)=0$]，而单位元是取值为 1 的常数函数 ε[即，对所有 $a\in\mathbb{R}$ 有 $\varepsilon(a)=1$].

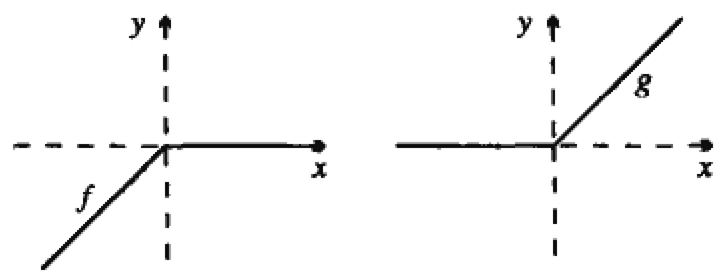


图 3-1 $\mathcal{F}(\mathbb{R})$不是整环

我们现在证明$\mathcal{F}(\mathbb{R})$不是整环. 定义 f 和 g 为

$$f(a)=\begin{cases} a & \text{当 } a\leqslant 0 \\ 0 & \text{当 } a\geqslant 0 \end{cases};\quad g(a)=\begin{cases} 0 & \text{当 } a\leqslant 0 \\ a & \text{当 } a\geqslant 0 \end{cases}$$

显然，f 和 g 都不是零(即，$f\neq z$，$g\neq z$). 另一方面，对每个 $a\in\mathbb{R}$ 有 $fg: a\mapsto f(a)g(a)=0$，这是因为 $f(a)$或 $g(a)$中至少有一个因子是数 0，由命题 2.2 知 $fg=z$. 因此$\mathcal{F}(\mathbb{R})$不是整环.

(ii)我们知道函数 f：$\mathbb{R}\to\mathbb{R}$ 是可微的当且仅当对所有 $a\in\mathbb{R}$，$f'(a)$存在. 令 $\mathcal{D}(\mathbb{R})=\{$所有可微函数 $f:\mathbb{R}\to\mathbb{R}\}$，我们断言$\mathcal{D}(\mathbb{R})$是$\mathcal{F}(\mathbb{R})$的子环. 因为 $\varepsilon'=z$，所以 $\varepsilon\in\mathcal{D}(\mathbb{R})$. 设 $f, g\in\mathcal{D}(\mathbb{R})$，因为$(f+g)'=f'+g'$，所以 $f+g\in\mathcal{D}(\mathbb{R})$，并且由导数的乘法法则知$(fg)'$存在. 因而$\mathcal{D}(\mathbb{R})$是$\mathcal{F}(\mathbb{R})$的子环，并由命题 3.9 知$\mathcal{D}(\mathbb{R})$构成环. ◀

→ **命题 3.12** (i)设 $m\geqslant 2$，则模 m 整数类$\mathbb{I}_m$ 是交换环.

(ii)交换环$\mathbb{I}_m$ 是整环当且仅当 m 是素数. 225

证明 (i)在定理 2.103 中，我们证明了在$\mathbb{I}_m$ 上定义的加法运算$[a+b]=[a]+[b]$满足交换环定义中的公理(i)到(iv)($[a]$是同余类$[a]=\{b\in\mathbb{Z}: b\equiv a \pmod m\}$). 在定理 2.105 中，我们证明了在$\mathbb{I}_m$ 上定义的乘法运算$[a][b]=[ab]$满足交换环定义中的公理(v)到(vii). 我们现在只需要证明分配律成立. 由于分配律在$\mathbb{Z}$ 中成立，所以有

$$\begin{aligned}[a]([b]+[c]) &= [a][b+c] \\ &= [a(b+c)]\end{aligned}$$

$$=[ab+ac]$$
$$=[ab]+[ac]$$
$$=[a][b]+[a][c].$$

因此，$\mathbb{I}_m$ 是交换环.（注意：若 $m=0$ 则 $\mathbb{I}_m=\mathbb{Z}$，若 $m=1$ 则 $\mathbb{I}_m$ 是零环.）

(ii)若 m 不是素数，则 $m=ab$，其中 $0<a$，$b<m$. 因为 m 不能整除 a，b，所以在 $\mathbb{I}_m$ 中 $[a]$和$[b]$都不等于$[0]$，但是$[a][b]=[m]=[0]$. 因此，$\mathbb{I}_m$ 不是整环.

反之，设 m 是素数. 因为 $m\geqslant 2$，所以$[1]\neq[0]$. 若$[a][b]=[0]$，则 $ab\equiv 0(\bmod m)$，即 $m\mid ab$. 由于 m 是素数，由欧几里得引理知 $m\mid a$ 或 $m\mid b$，即 $a\equiv 0(\bmod m)$或 $b\equiv 0(\bmod m)$，即$[a]=[0]$或$[b]=[0]$. 因此$\mathbb{I}_m$ 是整环. ■

环$\mathbb{I}_6$ 不是整环，这是因为$[2]\neq[0]$，$[3]\neq[0]$，但$[2][3]=[6]=[0]$.

交换环$\mathbb{Z}$ 的很多性质在更一般的情况下也成立. 我们现在把$\mathbb{Z}$ 中一些熟悉的概念推广到任意交换环上.

→ **定义** 设 a 和 b 是交换环 R 中的元素. 若存在元素 $c\in R$ 使得 $b=ca$，则称**在 R 中 a 整除 b**（或称 a 是 b 的一个**因子**，或称 b 是 a 的一个**倍数**），记为[⊖] $a\mid b$.

这里有一个极端的例子. 若 $0\mid a$，则存在某个 $b\in R$ 使 $a=0\cdot b$. 而 $0\cdot b=0$，我们必定有 $a=0$. 因此，$0\mid a$ 当且仅当 $a=0$.

注意：$a\mid b$ 是否成立不仅依赖于元素 a 和 b 而且也依赖于交换环 R. 例如，在$\mathbb{Q}$ 中 3 整除

226 2，这是因为 $2=3\times\frac{2}{3}$ 且 $\frac{2}{3}\in\mathbb{Q}$；另一方面，在$\mathbb{Z}$ 中 3 不能整除 2，这是因为不存在整数 c 使得 $3c=2$.

读者可以很快地验证以下每个事实. 对任意 $a\in R$，我们有 $a\mid a$，$1\mid a$，$-a\mid a$，$-1\mid a$ 和 $a\mid 0$.

引理 3.13 设 R 是交换环，并设 a，b，c 是 R 中的元素.

(i)若 $a\mid b$ 且 $b\mid c$，则 $a\mid c$.

(ii)若 $a\mid b$ 且 $a\mid c$，则 a 能整除 R 中形如 $sb+tc$ 的元素，其中 s，$t\in R$.

证明 留给读者作练习. ■

→ **定义** 设 R 是交换环，a，$b\in R$. R 中形如 $sa+tb$ 的元素称为 a，b 的**线性组合**，其中 s，$t\in R$.

因此，引理 3.13 是说 a，$b\in R$ 的任意公因数能整除 a，b 的任意线性组合.

→ **定义** 设 R 是交换环，$u\in R$. 若在 R 中 $u\mid 1$，即存在 $v\in R$ 使得 $uv=1$，则 u 称为 R 中的一个**单位**，其中 v 称为 u 的**逆元**（逆元的唯一性见习题 3.3），且通常记为 u^{-1}. 设 a，$r\in R$，若存在单位 $u\in R$ 使得 $a=ur$，则 a 称为 r 的**相伴元**.

→ **例 3.14** $\mathbb{Z}$ 中的单位仅有± 1，$n\in\mathbb{Z}$ 的相伴元是$\pm n$. ◀

我们对单位感兴趣，是因为总可以用它们去整除. 若 u 是 R 中的一个单位，则存在 $v\in R$ 使得 $uv=1$. 设 $a\in R$，因为

$$a=u(va)$$

⊖ 不要混淆了符号 $a\mid b$ 和 a/b. 第一个表示命题“a 是 b 的一个因子”，而另一个表示元素 $c\in R$ 满足 $bc=a$.

是 a 在 R 中的一个分解，所以 $u \mid a$. 因此，有充分理由定义商 $a/u=va=u^{-1}a$.（回忆一下，最后一个式子解释了为什么零不是 R 中的单位，即，为什么禁止用零去整除.）

正如整除性依赖于交换环 R 一样，元素 $u\in R$ 是否是单位也依赖于 R(因为有 $u \mid 1$ 在 R 中是否成立的问题). 例如，数 2 在$\mathbb{Q}$中是单位，这是因为$\frac{1}{2}$位于$\mathbb{Q}$中且 $2\times\frac{1}{2}=1$，但 2 在$\mathbb{Z}$中不是单位，因为不存在整数 v 使 $2v=1$.

下面的定理推广了习题 1.50. 227

命题 3.15 *设 R 是整环，a，$b\in R$ 不为零. 则 $a \mid b$ 且 $b \mid a$ 当且仅当存在某个单位 $u\in R$ 可使 $b=ua$.*

证明 若 $a \mid b$ 且 $b \mid a$，则存在元素 u，$v\in R$ 使得 $b=ua$，$a=vb$. 替换后得 $b=ua=uvb$. 由于 $b=1b$ 且 $b\neq 0$，所以由整环 R 中的消去律得 $1=uv$，所以 u 是单位.

反之，假设 $b=ua$，其中 u 是 R 中的单位. 显然 $a \mid b$. 因为存在 $v\in R$ 可使 $uv=1$，所以 $vb=vua=a$，这样 $b \mid a$. ■

存在一些交换环的例子，它们可说明命题 3.15 在交换环中不成立，所以在这个定理中假设 R 是整环是必要的.

$\mathbb{I}_m$ 中的单位是什么？

命题 3.16 *设 a 是一个整数，则$[a]$是$\mathbb{I}_m$ 中的单位当且仅当 a 和 m 互素. 实际上，若 $sa+tm=1$，则$[a]^{-1}=[s]$.*

证明 若$[a]$是$\mathbb{I}_m$ 中的单位，则存在$[s]\in\mathbb{I}_m$ 使得$[s][a]=[1]$. 因此，$sa\equiv 1(\bmod m)$，所以存在整数 t 使得 $sa-1=tm$，因而 $1=sa-tm$. 由习题 1.56 知 a 和 m 互素.

反之，若 a 和 m 互素，则存在整数 s，t 使得 $1=sa+tm$，因而 $sa-1=-tm$，$sa\equiv 1(\bmod m)$. 这样$[s][a]=[1]$，$[a]$是$\mathbb{I}_m$ 中的单位. ■

推论 3.17 *若 p 是素数，则$\mathbb{I}_p$ 中每个非零元$[a]$都是单位.*

证明 若$[a]\neq[0]$，则 $a\not\equiv 0(\bmod p)$，因而 $p\nmid a$. 又因为 p 是素数，所以 a 和 p 互素. ■

→ **记号** 设 R 是一个交换环，把 R 中的所有单位构成的子集记为

$$U(R)=\{R\text{ 中的所有单位}\}.$$

易验证 $U(R)$是一个乘法群，我们称 $U(R)$为 R **的单位群**. 由推论 3.17 知 $U(\mathbb{I}_m)=\{[a]\in\mathbb{I}_m:(a, m)=1\}$[我们已经在定理 2.109 的证明中见过 $U(\mathbb{I}_m)$].

交换环$\mathbb{I}_m$ 的引入使同余方程解的问题变得更加自然了. $\mathbb{Z}$ 中的同余方程 $ax\equiv b(\bmod m)$变为$\mathbb{I}_m$ 中的方程$[a][x]=[b]$. 若$[a]$是$\mathbb{I}_m$ 中的单位，即$(a, m)=1$，则它有逆元$[a]^{-1}=[s]$，于是我们可用它去整除，方程的解是$[x]=[a]^{-1}[b]=[s][b]=[sb]$. 换句话说，如果普通线性方程 $\alpha x=\beta$ 在$\mathbb{R}$ 中的解 $x=\alpha^{-1}\beta$ 得到了，则同余方程的解也就得到了. 228

习题

H 3.1 判断对错并说明理由.

(i)子集$\{r+s\pi: r, s\in\mathbb{Q}\}$是$\mathbb{R}$ 的一个子环.

(ii)一个整环的每个子环都是整环.

(iii)零环是$\mathbb{Z}$的一个子环.

(iv)存在无穷多个正整数m使得$\mathbb{I}_m$是一个整环.

(v)若S是交换环R的一个子环，则$U(S)$是$U(R)$的一个子群.

(vi)若S是交换环R的一个子环，则$U(S)=U(R)\cap S$.

(vii)若R是一个无限交换环，则$U(R)$是无限的.

(viii)若X是一个无限集，则X的所有有限子集构成的集合是布尔环$\mathcal{B}(X)$的一个子环.

3.2 证明交换环R有唯一的1，即，若对所有$r\in R$，$e\in R$满足$er=r$，则$e=1$.

*3.3 设R是一个交换环.

(i)证明加法消去律成立.

(ii)证明每个$a\in R$有唯一的加法逆元：若$a+b=0$和$a+c=0$，则$b=c$.

(iii)若$u\in R$是单位，证明它的逆元是唯一的：若$ub=1$和$uc=1$，则$b=c$.

3.4 (i)证明$\mathbb{Z}$中的减法不满足结合律.

(ii)举一个交换环R的例子，其减法满足结合律.

3.5 假设S是交换环R的一个子集，满足

(i)$1\in S$；

(ii)若a，$b\in S$，则$a+b\in S$；

(iii)若a，$b\in S$，则$ab\in S$.

(比较子环的定义，我们现在是假设$a+b\in S$而不是$a-b\in S$.)给出交换环R的一个例子，R包含一个这样的子集S，且S不是R的子环.

3.6 求$\mathbb{I}_{11}$中非零元素的乘法逆元.

*3.7 **H** (i)设X是一个集合，证明由X的子集构成的布尔群$\mathcal{B}(X)$[参见例2.47(viii)]带上对称差给出的加法运算$U+V=(U-V)\cup(V-U)$和乘法运算$UV=U\cap V$构成一个交换环. 我们称$\mathcal{B}(X)$为布尔环.

(ii)证明$\mathcal{B}(X)$恰含一个单位.

(iii)设Y是X的一个真子集，证明$\mathcal{B}(Y)$的单位元不等于$\mathcal{B}(X)$的单位元. 由此知$\mathcal{B}(Y)$不是$\mathcal{B}(X)$的子环.

(iv)证明每个$U\in\mathcal{B}(X)$满足$U^2=U$.

3.8 (i)设R是一个整环，$a\in R$满足$a^2=a$，证明$a=0$或$a=1$.

(ii)证明，例3.11(i)中的交换环$\mathcal{F}(\mathbb{R})$含有元素$f\neq 0$，1满足$f^2=f$.

229 3.9 求出例3.11(i)中交换环$\mathcal{F}(\mathbb{R})$的所有单位.

*3.10 把$\mathcal{F}(\mathbb{R})$的结构推广到集合X和任意交换环R上：设$\mathcal{F}(X,R)$是X到R的所有函数构成的集合，带上点加运算$f+g: x\mapsto f(x)+g(x)$和点乘运算$fg: x\mapsto f(x)g(x)$，$x\in X$.

(i)证明$\mathcal{F}(X,R)$是一个交换环.

(ii)证明，若X至少有两个元素，则$\mathcal{F}(X,R)$不是一个整环.

(iii)若R是一个交换环，则记$\mathcal{F}(R,R)$为$\mathcal{F}(R)$：

$$\mathcal{F}(R)=\{所有函数\ R\to R\}.$$

证明$\mathcal{F}(\mathbb{I}_2)$只含有四个元素，并且对任意$f\in\mathcal{F}(\mathbb{I}_2)$有$f+f=0$.

*3.11 **H** (i)证明交换环$\mathbb{C}$是一个整环.

(ii)证明$\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$都是整环.

(iii)证明高斯整数环是一个整环.

*3.12 证明交换环 R 的任一族子环的交是 R 的一个子环.

H 3.13 证明，Z 的子环只有本身.

H 3.14 设 a 和 m 是互素的整数. 证明，若 $sa+tm=1=s'a+t'm$，则 $s\equiv s' \pmod m$. 参见习题 1.56.

3.15 H (i) $R=\{a+b\sqrt{2}: a, b\in \mathbb{Z}\}$ 是一个整环吗？

H (ii) $R=\left\{\frac{1}{2}(a+b\sqrt{2}): a, b\in \mathbb{Z}\right\}$ 是一个整环吗？

(iii) 利用 $\alpha=\frac{1}{2}(1+\sqrt{-19})$ 是 x^2-x+5 的根，证明 $R=\{a+b\alpha: a, b\in \mathbb{Z}\}$ 是一个整环.

3.16 证明所有 C^∞-函数构成的集合是 $\mathcal{F}(\mathbb{R})$ 的一个子环.（见习题 1.42.）

→3.2 域

$\mathbb{Q}$ 和 $\mathbb{Z}$ 之间有一个明显的不同：$\mathbb{Q}$ 中每个非零元素都是单位.

→ **定义** 若交换环 F 满足 $1\neq 0$ 且每个非零元素 a 都是单位，即存在 $a^{-1}\in F$ 使得 $a^{-1}a=1$，则 F 称为**域**[⊖]

$\mathbb{Q}$，$\mathbb{R}$ 和 $\mathbb{C}$ 都是域.

可以根据单位群的概念来重新叙述域的定义. 交换环 R 是域当且仅当 $U(R)=R^\times$，其中 $R^\times$ 是由 R 的非零元素构成的集合. 换句话说，R 是域当且仅当 $R^\times$ 是一个乘法群. 230

命题 3.18 每个域 F 都是整环.

证明 假设 $ab=ac$，其中 $a\neq 0$. 两边乘以 a^{-1} 得 $a^{-1}ab=a^{-1}ac$，所以 $b=c$. ■

当然，该命题的逆命题不成立，因为 $\mathbb{Z}$ 是整环但不是域.

→ **命题 3.19** 交换环 $\mathbb{I}_m$ 是域当且仅当 m 是素数.

证明 若 m 是素数，则由推论 3.17 知 $\mathbb{I}_m$ 是域.

反之，若 m 是合数，则由命题 3.12 知 $\mathbb{I}_m$ 不是整环. 又由命题 3.18 知 $\mathbb{I}_m$ 不是域，矛盾. ■

记号 当 p 是素数时，我们通常把域 $\mathbb{I}_p$ 记为

$$\mathbb{F}_p.$$

在本章的结尾处，我们将证明除 $\mathbb{F}_p$ 之外还有其他的有限域（习题 3.19 构造了一个含 4 个元素的域）.

当我还是研究生时，我的一位同学被聘请去给一个有数学天赋的 10 岁男孩做家庭教师. 为说明这个孩子有很高的天赋，这位家庭教师讲述了他教 2×2 矩阵以及矩阵乘法的那个学期. 当他用单位矩阵展示矩阵乘法时，孩子眼睛一亮，立刻独自去一个角落. 几分钟后，他告诉老师矩阵 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 有逆元当且仅当 $ad-bc\neq 0$！

在另一个学期，孩子学习了域的定义. 当有理数、实数和复数等一些熟悉的例子展示出来时，孩子感到非常满意. 但是当给出一个只有 2 个元素的域时，他变得十分激动. 在仔细检验

⊖ 英语术语“域(field)”(穆尔(E. H. Moore)在 1893 年写的一篇关于分类有限域的文章中首先使用了该术语)在数学上的衍生用法同德语术语 Körper 和法语术语 corps 在数学上的衍生用法与单词“群(group)”和“环(ring)”的衍生用法是十分相似的：每个单词分别表示一个“领域”，“一组”事物或“事物的全体”. 单词“整环(domain)”是英语词语“整数领域(integral domain)”的缩写，而这个词则是来自德语 Integretätsbereich，指类似于整数的事物的集合.

每个公理确实都成立后，他疯狂地探索起来．我讲这个故事是为了说明有限域是非常令人惊奇和出乎意料的．

在第 2 章中，我们介绍了$\mathbb{R}$中非奇异矩阵群 $GL(2, \mathbb{R})$．之后，我们看到$\mathbb{R}$被$\mathbb{Q}$或$\mathbb{C}$取代后还是群．现在我们看到$\mathbb{R}$可以被任意域 k 取代：对每个域 k，$GL(2, k)$都是一个群．特别地，对每个素数 p，$GL(2, \mathbb{F}_p)$是一个有限群．

习题 3.11 表明，整环的每个子环本身是一个整环．由于域都是整环，所以域的每个子环都是整环．这道习题的逆命题也成立，且更有趣：每个整环都是域的子环．

给定域 F 中的四个元素 a，b，c，d，其中 $b\neq 0$，$d\neq 0$，并假设 $ab^{-1}=cd^{-1}$．两边乘以 bd 得 $ad=bc$．换句话说，若把 ab^{-1}写作 a/b，则我们刚好证明了 $a/b=c/d$ 可推出 $ad=bc$，即"叉
231 乘"是正确的．反之，若 $ad=bc$，且 b 和 d 都不为零，则乘以 $b^{-1}d^{-1}$ 得 $ab^{-1}=cd^{-1}$，即 $a/b=c/d$．例 2.17(iii)告诉我们叉乘是$\{(a, b)\in\mathbb{Z}\times\mathbb{Z} : b\neq 0\}$上的一个等价关系，我们现在来推广该结论．

引理 3.20 *设 R 是一个整环，$X=\{(a, b)\in R\times R : b\neq 0\}$，用叉乘定义 X 上的一个关系：$(a, b)\equiv(c, d)$ 当且仅当 $ad=bc$，则该关系是一个等价关系．*

证明 自反性和对称性易验证．对于传递性，假设$(a, b)\equiv(c, d)$，$(c, d)\equiv(e, f)$．由 $ad=bc$ 得 $adf=bcf$，由 $cf=de$ 得 $bcf=bde$，因此 $adf=bde$．由于 R 是整环，所以我们可以消去非零元 d 得 $af=be$，即$(a, b)\equiv(e, f)$． ■

下面定理的证明是由整数整环$\mathbb{Z}$来构造有理数域$\mathbb{Q}$的标准方法的一个自然推广．

→ **定理 3.21** *若 R 是整环，则存在包含 R 作为子环的一个域 F．而且，可以使 F 满足：对每个 $f\in F$，存在 a，$b\in R$ 使 $f=ab^{-1}$ 且 $b\neq 0$．*

证明 由引理 3.20 知，叉乘[即$(a, b)\equiv(c, d)$当且仅当 $ad=bc$]是 $X=R\times R^{\times}$ 上的一个等价关系．$(a, b)\in X$ 的等价类记为$[a, b]$，定义 F 为所有这样的等价类构成的集合．给 F 带上下述加法和乘法运算(若我们假设$[a, b]$是分数 a/b，则这些都是普通公式)：

$$[a,b]+[c,d]=[ad+bc,bd],$$
$$[a,b][c,d]=[ac,bd].$$

注意，因为 R 是一个整环，所以由 $b\neq 0$ 和 $d\neq 0$ 可推出 $bd\neq 0$，因此右边的符号是有意义的．现在 F 是域的证明只是一系列的验证了．

加法 $F\times F\to F$ 是定义良好的：若$[a, b]=[a', b']$，$[c, d]=[c', d']$，则$[ad+bc, bd]=[a'd'+b'c', b'd']$．因为 $ab'=a'b$，$cd'=c'd$，所以

$$\begin{aligned}(ad+bc)b'd' &= adb'd'+bcb'd'=(ab')dd'+bb'(cd')\\ &= a'bdd'+bb'c'd=(a'd'+b'c')bd,\end{aligned}$$

即$(ad+bc, bd)\equiv(a'd'+b'c', b'd')$，这正是我们所要的．类似的计算可证明乘法 $F\times F\to F$ 也是定义良好的．

F 是交换环的证明也是按章行事，留给读者去证明，但读者要注意：零元素是$[0, 1]$，单
232 位元是$[1, 1]$，$[a, b]$的负数是$[-a, b]$．若我们把 $a\in R$ 和$[a, 1]\in F$ 看成是相同的，则易见所有这样的元素构成的族 R'是 F 的一个子环：

$$[1,1] \in R';$$
$$[a,1]-[c,1] = [a,1]+[-c,1] = [a-c,1] \in R';$$
$$[a,1][c,1] = [ac,1] \in R'.$$

为证明 F 是一个域，首先观察到若 $[a, b]\neq 0$，则 $a\neq 0$（因为 F 的零元素是 $[0, 1]=[0, b]$）. $[a, b]$ 的逆元是 $[b, a]$，这是因为 $[a, b][b, a]=[ab, ab]=[1, 1]$.

最后，若 $b\neq 0$，则 $[1, b]=[b, 1]^{-1}$（正如我们刚才所看到的）. 因此，若 $[a, b]\in F$，则 $[a, b]=[a, 1][1, b]=[a, 1][b, 1]^{-1}$. 证明可以结束了，因为 $[a, 1]$，$[b, 1]\in R'$. ■

定理 3.21 的叙述不够精确. 域 F 不能把 R 作为其子环，因为 R 根本不是 F 的子集. 代替地，我们证明了 F 包含子环 $R'=\{[a, 1]: a\in R\}$，它具有我们想得到的性质. R' 非常类似于 R，我们一旦介绍了同构的概念（见例 3.31），就能够把 R' 和 R 等同起来.

→ **定义** 由定理 3.21 中的整环 R 构造的域 F 称为 R 的**分式域**，我们记它为

$$\mathrm{Frac}(R),$$

并记元素 $[a, b]\in \mathrm{Frac}(R)$ 为 a/b. 特别地，R' 的元素 $[a, 1]$ 记为 $a/1$，或简单地记为 a.

注意，$\mathbb{Z}$ 的分式域是 $\mathbb{Q}$，即 $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$. 在下一节中，我们将看到：若 k 是域，则所有系数取自 k 的多项式 $f(x)$ 构成的集合作成一个整环，记为 $k[x]$. $\mathrm{Frac}(k[x])$ 的元素 $f(x)/g(x)$ 通常被称为**有理函数**.

→ **定义** 若域 K 的子环 k 也是域，则 k 称为域 K 的**子域**.

→ **命题 3.22** (i) 域 K 的子集 k 是子域当且仅当 k 是子环且它在逆元下是封闭的，即，若 $a\in k$，$a\neq 0$，则 $a^{-1}\in k$.

(ii) 若 $\{F_i: i\in I\}$ 是域 K 的子域族（可能无限个），则 $k=\bigcap_{i\in I} F_i$ 是 K 的子域. 233

证明 (i) 若域 K 的子集 k 是子域，则显然 k 包含它的非零元素的逆元. 反之，若 k 是子环且包含它的非零元素的逆元，则它是域，因而它是 K 的子域.

(ii) 利用 (i). 由习题 3.12 知子环的任意交集还是子环，所以 k 是 K 的子环. 若 $a\in k$ 是非零元素，则 a 属于每个 F_i. 又因为 F_i 是子域，所以 $a^{-1}\in F_i$，所以 $a^{-1}\in\bigcap_i F_i=k$. 这样 k 是 K 的子域. ■

→ **定义** 若 K 是域，则 K 的所有子域的交集 k 称为 K 的**素域**.

当然，每个域都有唯一的素域. 在命题 3.110 中，我们将看到：每个素域在本质上都等于 $\mathbb{Q}$ 或 $\mathbb{F}_p$（p 为某个素数）.

习题

H 3.17 判断对错并说明理由.

(i) 每个域都是一个整环.

(ii) 存在一个有限域，其元素个数超过 10^{100}.

(iii) 若 R 是一个整环，则存在包含 R 的唯一域.

(iv) 每个交换环是一个域的子环.

(v) 子集 $R=\mathbb{Q}[i]=\{a+bi: a, b\in\mathbb{Q}\}$ 是 $\mathbb{C}$ 的一个子域.

(vi) $\mathbb{Q}[i]=\{a+bi: a, b\in\mathbb{Q}\}$ 的素域是 $\mathbb{Q}$.

(vii)若 $R=\mathbb{Q}[\sqrt{2}]$，则 $\mathrm{Frac}(R)=\mathbb{R}$.

3.18 (i)设 R 是交换环，定义**圈运算** $a\circ b$ 为

$$a\circ b=a+b-ab.$$

证明，圈运算满足结合律，并且对所有 $a\in R$ 有 $0\circ a=a$.

(ii)证明，交换环 R 是一个域当且仅当集合

$$R^{\#}=\{r\in R: r\neq 1\}$$

在圈运算下作成阿贝尔群.

*3.19 (狄恩，R. A. Dean)定义 $\mathbb{F}_4$ 为所有如下 2×2 矩阵构成的集合

$$\mathbb{F}_4=\left\{\begin{bmatrix}a & b\\ b & a+b\end{bmatrix}: a,b\in\mathbb{F}_2\right\}.$$

(i)证明，$\mathbb{F}_4$ 是一个交换环，其运算是矩阵加法和矩阵乘法.

(ii)证明，$\mathbb{F}_4$ 是仅有四个元素的域.

234 (iii)证明，$\mathbb{I}_4$ 不是域.

H 3.20 证明，元素个数有限的整环都是域. 利用命题 3.12，这个结论给出命题 3.19 充分性的一个新的证法.

*H 3.21 求高斯整数环 $\mathbb{Z}[i]$ 的所有单位.

3.22 证明，$F=\{a+b\sqrt{2}: a, b\in\mathbb{Q}\}$ 是一个域.

*3.23 (i)证明，$F=\{a+bi: a, b\in\mathbb{Q}\}$ 是一个域.

(ii)证明，每个 $u\in F$ 有分解式 $u=\alpha\beta^{-1}$，其中 $\alpha, \beta\in\mathbb{Z}[i]$. (看习题 3.50(ii).)

*3.24 设 R 是一个交换环，定义 R 上的关系≡：$a\equiv b$ 当且仅当存在单位 $u\in R$ 使得 $b=ua$.

(i)证明≡是一个等价关系.

(ii)证明，若 $a\equiv b$，则 $(a)=(b)$，其中 $(a)=\{ra: r\in R\}$. 反之，证明，若 R 是一个整环，则由 $(a)=(b)$ 可推出 $a\equiv b$.

3.25 若 R 是一个整环，证明不存在 $\mathrm{Frac}(R)$ 的子域 K 满足

$$R\subseteq K\subsetneq \mathrm{Frac}(R).$$

*3.26 设 k 是一个域，R 是子环

$$R=\{n\cdot 1: n\in\mathbb{Z}\}\subseteq k.$$

(i)若 F 是 k 的一个子域，证明 $R\subseteq F$.

(ii)证明，k 的子域 F 是 k 的素域当且仅当它是 k 的包含 R 的最小子域，即不存在满足 $R\subseteq F'\subsetneq F$ 的子域 F'.

(iii)若 R 是 k 的一个子域，证明 R 是 k 的素域.

3.27 (i)证明 $\mathbb{C}$ 的每个子域都包含 $\mathbb{Q}$.

(ii)证明 $\mathbb{R}$ 的素域是 $\mathbb{Q}$.

(iii)证明 $\mathbb{C}$ 的素域是 $\mathbb{Q}$.

*3.28 H (i)对任意域 F，证明 $\Sigma(2, F)\cong \mathrm{Aff}(1, F)$，其中 $\Sigma(2, F)$ 表示随机群(其定义在习题 2.48 中).

(ii)若 F 是一个有限域，含有 q 个元素，证明 $|\Sigma(2, F)|=q(q-1)$.

(iii)证明 $\Sigma(2, \mathbb{F}_3)\cong S_3$.

→3.3 多项式

尽管读者十分熟悉多项式，但我们还要进一步仔细地介绍它们，以便读者不再对"未知量" x 感到神秘.

非正式地，多项式是指形如 $s_0+s_1x+s_2x^2+\cdots+s_nx^n$ 的一个"表达式"．关键之处在于我们应当注意多项式的系数 s_0，s_1，s_2，…，s_n 取自哪里． 235

→ **定义** 设 R 是一个交换环，则称函数 $\sigma:\mathbb{N}\to R$ 为 R 上的一个**形式幂级数**．作为任意函数，一个形式幂级数 $\sigma:\mathbb{N}\to R$ 可以由其值确定，对每个 $i\in\mathbb{N}$，记 $\sigma(i)=s_i\in R$，因此

$$\sigma=(s_0,s_1,s_2,\cdots,s_i,\cdots).$$

称值 $s_i\in R$ 为该形式[⊖]幂级数的**系数**[⊜]．

由命题 2.2 知，R 上的两个形式幂级数 σ 和 τ 相等当且仅当它们的系数相匹配，即对所有 $i\geqslant 0$ 有 $\sigma(i)=\tau(i)$．

→ **定义** 交换环 R 上的一个形式幂级数 $\sigma=(s_0$，s_1，…，s_i，…$)$ 称为 R 上的一个**多项式**，若存在整数 $n\geqslant 0$，使得对所有 $i>n$ 有 $s_i=0$，即

$$\sigma=(s_0,s_1,\cdots,s_n,0,0,\cdots).$$

一个多项式只有有限个非零系数，然而一个形式幂级数可能有无穷个非零系数．

→ **定义** **零多项式** 0 是指所有系数均为零的多项式$(0, 0, 0, \cdots)$．若 $\sigma=(s_0$，s_1，…，s_n，0，0，…$)$是一个非零多项式，则存在自然数 n 满足 $s_n\neq 0$ 且对所有 $i>n$ 有 $s_i=0$．我们称 s_n 为 σ 的**首项系数**，称 n 为 σ 的**次数**[⊜⊜]，并记次数 n 为 $\deg(\sigma)$．

零多项式 0 没有次数，因为它没有非零系数．其他任意多项式都有次数．

记号 若 R 是交换环，则所有系数取自 R 的多项式构成的集合记为 $R[x]$．

给 $R[x]$带上下列运算．定义

$$\sigma+\tau=(s_0+t_0,s_1+t_1,\cdots,s_i+t_i,\cdots)$$

和

$$\sigma\tau=(a_0,a_1,\cdots,a_k,\cdots),$$ 236

其中 $a_k=\sum_{i+j=k}s_it_j=\sum_{i=0}^{k}s_it_{k-i}$．因此，

$$\sigma\tau=(s_0t_0,s_0t_1+s_1t_0,s_0t_2+s_1t_1+s_2t_0,\cdots).$$

下列命题将告诉我们该乘法公式来自于哪里．

命题 3.23 若 R 是交换环，且 r，s_i，$t_j\in R$，$i\geqslant 0$，$j\geqslant 0$，则

$$(s_0+s_1r+\cdots)(t_0+t_1r+\cdots)=a_0+a_1r+\cdots+a_kr^k+\cdots,$$

其中对所有 $k\geqslant 0$ 有 $a_k=\sum_{i+j=k}s_it_j$．

注 对 $k\geqslant 0$ 用归纳法证明，但因为思路是很清楚的，所以我们只给出一个非正式的证明．

⊖ 我们通常把形式幂级数 $\sigma=(s_0, s_1, s_2, \cdots, s_i, \cdots)$记为 $s_0+s_1x+s_2x^2+\cdots=\sum_{i=0}^{\infty}s_ix^i$．使用形容词"形式"是因为这里不存在收敛的概念．实际上，即使 $R=\mathbb{R}$，使得收敛的概念有意义，所有收敛幂级数的集合也只是$\mathbb{R}$上所有形式幂级数集合的真子集．

⊜ "系数"的含义是"一起作用到达一个单一的终点"．这里，系数合起来确定一个形式幂级数．

⊜⊜ 术语"次数"来自意为"台阶"的一个拉丁词．

证明 记 $\sum_i s_i r^i = f(r)$，$\sum_j t_j r^j = g(r)$. 则

$$\begin{aligned} f(r)g(r) &= (s_0 + s_1 r + s_2 r^2 + \cdots)g(r) = s_0 g(r) + s_1 r g(r) + s_2 r^2 g(r) + \cdots \\ &= s_0(t_0 + t_1 r + \cdots) + s_1 r(t_0 + t_1 r + \cdots) + s_2 r^2(t_0 + t_1 r + \cdots) + \cdots \\ &= s_0 t_0 + (s_1 t_0 + s_0 t_1)r + (s_2 t_0 + s_1 t_1 + s_0 t_2)r^2 + \\ &\quad (s_0 t_3 + s_1 t_2 + s_2 t_1 + s_3 t_0)r^3 + \cdots. \end{aligned}$$

■

→ **引理 3.24** *设 R 是一个交换环，并设 σ，$\tau \in R[x]$是非零多项式.*

(i)$\sigma\tau=0$ 或 $\deg(\sigma\tau) \leqslant \deg(\sigma)+\deg(\tau)$.

(ii)*若 R 是整环，则 $\sigma\tau \neq 0$ 且*

$$\deg(\sigma\tau) = \deg(\sigma) + \deg(\tau).$$

证明 (i)设 $\sigma=(s_0, s_1, \cdots)$的次数为 m，$\tau=(t_0, t_1, \cdots)$的次数为 n，并设 $\sigma\tau=(a_0, a_1, \cdots)$. 只需证明对所有 $k>m+n$ 有 $a_k=0$. 根据定义，

$$a_k = \sum_{i+j=k} s_i t_j.$$

若 $i \leqslant m$，则 $j=k-i \geqslant k-m>n$(因为 $k>m+n$)，所以 $t_j=0$(因为 τ 的次数为 n). 若 $i>m$，则

237 $s_i=0$，这是因为 σ 的次数为 m. 不管哪种情形都有每一项 $s_i t_j=0$，所以$a_k = \sum_{i+j=k} s_i t_j = 0$.

(ii) 现设 $k = m+n$. 由与(i) 相同的计算可知，除了 $s_m t_n$(σ 和 τ 的首项系数的积) 可能例外之外，a_{m+n} 中的每一项 $s_i t_j$ 都是 0：

$$s_0 t_{m+n} = \cdots = s_{n-1} t_{m+1} = 0 = s_{n+1} t_{m-1} = \cdots = s_{m+n} t_0.$$

若 $i<m$，则 $m-i>0$，因而 $j=m-i+n>n$，所以 $t_j=0$；若 $i>m$，则 $s_i=0$. 因而

$$a_{m+n} = s_m t_n.$$

由于 R 是整环，所以由 $s_m \neq 0$ 和 $t_n \neq 0$ 可知 $s_m t_n \neq 0$，因而 $\sigma\tau \neq 0$ 且 $\deg(\sigma\tau)=m+n=\deg(\sigma)+\deg(\tau)$. ■

→ **命题 3.25** (i)*若 R 是交换环，则 $R[x]$是包含 R 作为子环的交换环.*

(ii)*若 R 是整环，则 $R[x]$也是整环.*

证明 (i)加法和乘法是 $R[x]$上的两个运算：两个多项式 σ，τ 的和是一个多项式[实际上，$\sigma+\tau=0$ 或 $\deg(\sigma+\tau) \leqslant \max\{\deg(\sigma), \deg(\tau)\}$]，而由引理 3.24 知，两个多项式的积也是一个多项式. 我们照例要验证交换环的所有公理，这项任务留给读者. 注意，公理中的 0 是零多项式，1 是多项式(1，0，0，…)，$(s_0, s_1, \cdots, s_i, \cdots)$的负元是$(-s_0, -s_1, \cdots, -s_i, \cdots)$. 仅有的问题是证明乘法结合律，我们提示一下：若 $\rho=(r_0, r_1, \cdots, r_i, \cdots)$，则多项式 $\rho(\sigma\tau)$ 的第 ℓ 个系数是 $\sum_{i+j+k=\ell} r_i(s_j t_k)$，而$(\rho\sigma)\tau$的第$\ell$个系数是 $\sum_{i+j+k=\ell}(r_i s_j)t_k$，两者相等，这是因为 R 中的乘法满足结合律.

易检验 $R'=\{(r, 0, 0, \cdots): r \in R\}$是 $R[x]$的一个子环，我们把 $r \in R$ 与$(r, 0, 0, \cdots)$看作是相等的，从而把 R'与 R 看作是相等的.

(ii)若 R 是整环且σ，τ 是非零多项式，则由引理 3.24 知 $\sigma\tau \neq 0$，因而 $R[x]$是整环. ■

→ **定义** *若 R 是交换环，则 $R[x]$称为 R 上的***多项式环**.

如同断言整环是它的分式域的子环不完全正确一样(在定理 3.21 中)，我们断言一个交换环 R 是 $R[x]$ 的子环也是不完全正确的. 我们已经证明了 $R[x]$ 真的包含有一个子环，即 $R'=\{(r, 0, 0, \cdots): r\in R\}$，它十分相似于 R. 我们一旦介绍了同构的概念，就可以把 R' 和 R 等同起来(见例 3.31). 238

→ **定义** 定义未定元为元素

$$x=(0,1,0,0,\cdots)\in R[x].$$

虽然 x 既不是"未知量"也不是一个变量，但我们还是叫它未定元. 未定元 x 是环 $R[x]$ 中的特殊元素，即多项式 $(s_0, s_1, s_2, \cdots)$，其中 $s_1=1$，其他所有 $s_i=0$. 我们坚持认为交换环有一个单位，这样才有未定元的概念. 若所有偶数构成的集合 E 是交换环，则 $E[x]$ 不包含 x (但包含 $2x$). 注意，若 R 是零环，则 $R[x]$ 也是零环.

引理 3.26 (i)若 $\sigma=(s_0, s_1, \cdots, s_j, \cdots)$，则

$$x\sigma=(0,s_0,s_1,\cdots,s_j,\cdots);$$

即用 x 去乘可使每个系数向右移动一步.

(ii)若 $n\geqslant 1$，则 x^n 是第 n 个系数为 1 而其他所有系数为 0 的多项式.

(iii)若 $r\in R$，则

$$(r,0,0,\cdots)(s_0,s_1,\cdots,s_j,\cdots)=(rs_0,rs_1,\cdots,rs_j,\cdots).$$

证明 (i)记 $x=(t_0, t_1, \cdots, t_i, \cdots)$，其中 $t_1=1$，其他所有 $t_i=0$，并设 $x\sigma=(a_0, a_1, \cdots, a_k, \cdots)$. 因为 $t_0=0$，所以 $a_0=t_0s_0=0$. 若 $k\geqslant 1$，则 $a_k=\sum_{i+j=k}s_it_j$ 中的非零项只有 $s_{k-1}t_1=s_{k-1}$，这是因为 $t_1=1$，对 $i\neq 1$，$t_i=0$. 因此，对 $k\geqslant 1$，$x\sigma$ 的第 k 个系数 a_k 是 s_{k-1}，且 $x\sigma=(0, s_0, s_1, \cdots, s_i, \cdots)$.

(ii)利用(i)，用归纳法易得.

(iii)由乘法的定义易得. ■

若我们把 $(r, 0, 0, \cdots)$ 和 r 等同起来，则引理 3.26(iii)叙述为

$$r(s_0,s_1,\cdots,s_i,\cdots)=(rs_0,rs_1,\cdots,rs_i,\cdots).$$

我们现在可以用回普通记号.

→ **命题 3.27** 若 $\sigma=(s_0, s_1, \cdots, s_n, 0, 0, \cdots)$，则

$$\sigma=s_0+s_1x+s_2x^2+\cdots+s_nx^n,$$

其中每个元素 $s\in R$ 被看作与多项式 $(s, 0, 0, \cdots)$ 相等. 239

证明

$$\begin{aligned}\sigma&=(s_0,s_1,\cdots,s_n,0,0,\cdots)\\&=(s_0,0,0,\cdots)+(0,s_1,0,\cdots)+\cdots+(0,0,\cdots,s_n,0,\cdots)\\&=s_0(1,0,0,\cdots)+s_1(0,1,0,\cdots)+\cdots+s_n(0,0,\cdots,1,0,\cdots)\\&=s_0+s_1x+s_2x^2+\cdots+s_nx^n.\end{aligned}$$ ■

从现在开始，我们将使用这个熟悉的(且标准的)记号. 根据习惯，我们将写

$$f(x)=s_0+s_1x+s_2x^2+\cdots+s_nx^n$$

而不写 $\sigma=(s_0, s_1, \cdots, s_n, 0, 0, \cdots)$.

这里有一些与多项式相关的标准词汇. 若 $f(x)=s_0+s_1x+s_2x^2+\cdots+s_nx^n$，其中 $s_n\neq0$，则称 s_0 为**常数项**，正如我们已经说过的，称 s_n 为首项系数. 若首项系数 $s_n=1$，则称 $f(x)$ 为**首一多项式**. 除零多项式 0（所有系数为 0）之外，其他多项式都有次数. **常数多项式**是指零多项式或次数为 0 的多项式. 次数为 1 的多项式，即 $a+bx$，$b\neq0$，称为**线性多项式**，次数为 2 的多项式称为**二次多项式**[⊖]，次数为 3 的多项式称为**三次多项式**，等等.

→ **推论 3.28** *多项式 $f(x)=s_0+s_1x+s_2x^2+\cdots+s_nx^n$ 和多项式 $g(x)=t_0+t_1x+t_2x^2+\cdots+t_mx^m$ 相等，当且仅当对所有 $i\in\mathbb{N}$ 有 $s_i=t_i$.*

证明 我们只需用熟悉的记号重述多项式相等的定义即可. ■

我们现在可以把未定元 x 看作一个变量，这是 x 通常扮演的角色. 若 R 是交换环，对多项式 $f(x)=s_0+s_1x+s_2x^2+\cdots+s_nx^n\in R[x]$赋值，则可以定义一个**多项式函数** $f^\flat: R\to R$：若 $r\in R$，定义 $f^\flat(r)=s_0+s_1r+s_2r^2+\cdots+s_nr^n\in R$[通常我们不会这么繁琐，而是把 $f^\flat(r)$ 写为 $f(r)$]. 读者应当认识到多项式和多项式函数是不同的两个对象. 例如，若 R 是一个有限环（例如$\mathbb{I}_m$），则 R 到自身的函数只有有限个，所以只有有限个多项式函数. 另一方面，若 R 是非零环，则存在无穷多个多项式. 例如，由推论 3.28 知，所有幂 1，x，x^2，…，x^n，…都是

240 互不相同的.

→ **定义** *设 k 是域，则把 $k[x]$的分式域 $\mathrm{Frac}(k[x])$记为 $k(x)$，称之为 k 上的**函数域**. 称 $k(x)$的元素为 k 上的**有理函数**.*

命题 3.29 *函数域 $k(x)$的元素形如 $f(x)/g(x)$，其中 $f(x)$，$g(x)\in k[x]$且 $g(x)\neq0$.*

证明 因为函数域是分式域，所以由定理 3.21 知 $k(x)$中的每个元素有形式 $f(x)g(x)^{-1}$. ■

命题 3.30 *若 p 是素数，则函数域$\mathbb{F}_p(x)$是一个无限域，其素域是$\mathbb{F}_p$.*

证明 由命题 3.25 知，$\mathbb{F}_p[x]$是一个整环. 它的分式域$\mathbb{F}_p(x)$是以$\mathbb{F}_p[x]$为子环的一个域，再由命题 3.25 知$\mathbb{F}_p[x]$以$\mathbb{F}_p$ 为子环. 这样由习题 3.26 知$\mathbb{F}_p$ 是素域. ■

尽管多项式和多项式函数是不同的(我们将在推论 3.52 中看到，当系数环 R 是无限域时，它们是相同的)，我们通常称 $R[x]$为 R 上关于一个变量(或未定元)的所有多项式构成的环. 若记 $A=R[x]$，则多项式环 $A[y]$称为 R 上关于两个变量(或未定元)x 和 y 的所有多项式构成的环，记为 $R[x, y]$. 例如，二次多项式 $ax^2+bxy+cy^2+dx+ey+f$ 可记为 $cy^2+(bx+e)y+(ax^2+dx+f)$，是系数在 $R[x]$中关于 y 的多项式. 根据归纳法，我们可以构造交换环 $R[x_1, x_2, \cdots, x_n]$，它是由系数在 R 中关于 n 个变量(或未定元)的所有多项式构成的. 对 n 用归纳法可将命题 3.25 推广：若 R 是整环，则 $R[x_1, x_2, \cdots, x_n]$也是整环. 而且，当 F 是域时，我们可以把 $\mathrm{Frac}(F[x_1, x_2, \cdots, x_n])$描述成关于 n 个变量(或未定元)的所有有理函数集，记为 $F(x_1, x_2, \cdots, x_n)$，其元素有形式 $f(x_1, x_2, \cdots, x_n)/g(x_1, x_2, \cdots, x_n)$，其中 f，$g\in F[x_1, x_2, \cdots, x_n]$.

⊖ 之所以称为二次多项式，是因为特殊的二次式 x^2 给出了正方形的面积. 类似地，之所以称为三次多项式，是因为 x^3给出了正方体的体积. 之所以称为线性多项式，是因为$\mathbb{R}[x]$中线性多项式的图形是一条直线.

习题

H 3.29 判断对错并说明理由.

(i) x^3-2x+5 的序列记号是 $(5,-2,0,1,0,\cdots)$.

(ii) 若 R 是一个整环，则 $R[x]$ 是一个整环.

(iii) $\mathbb{Q}[x]$ 是一个域.

(iv) 若 k 是一个域，则 $k[x]$ 的素域是 k.

(v) 若 R 是一个整环，且 $f(x), g(x)\in R[x]$ 都非零，则 $\deg(fg)=\deg(f)+\deg(g)$. 241

(vi) 若 R 是一个整环，且 $f(x), g(x)\in R[x]$ 都非零，则 $f(x)+g(x)=0$ 或 $\deg(f+g)\leqslant\max\{\deg(f),\deg(g)\}$.

(vii) 若 k 是一个域，则 $k[x]=k(x)$.

H 3.30 证明，若 R 是一个非零交换环，则 $R[x]$ 不是域.

*3.31 设 k 是一个域，A 表示 k 上的 $n\times n$ 矩阵(所以幂 A^i 有定义). 若 $f(x)=c_0+c_1x+\cdots+c_mx^m\in k[x]$，则定义

$$f(A)=c_0I+c_1A+\cdots+c_mA^m.$$

(i) 证明，$k[A]=\{f(A): f(x)\in k[x]\}$ 在矩阵加法和矩阵乘法下作成一个交换环.

(ii) 若 $f(x)=p(x)q(x)\in k[x]$，且 A 是 k 上的 $n\times n$ 矩阵，证明 $f(A)=p(A)q(A)$.

(iii) 给出 $n\times n$ 矩阵 A 和 B 的例子，使得 $k[A]$ 是一个整环而 $k[B]$ 不是整环.

*3.32 H (i) 设 R 是一个整环. 证明，$f(x)\in R[x]$ 是 $R[x]$ 中的单位当且仅当 $f(x)$ 是一个非零常数且是 R 中的单位.

(ii) 证明，$\mathbb{I}_4[x]$ 中 $([2]x+[1])^2=[1]$ 成立. 由此知，(i) 中的命题对不为整环的交换环不成立. [若对某个整数 $m\geqslant 1$ 有 $z^m=0$，则称 $z\in R$ 为幂零的. 对任意交换环 R，可以证明多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$ 是 $R[x]$ 中的单位当且仅当 a_0 是 R 中的单位且对所有 $i\geqslant 1$，a_i 是幂零的.]

*H 3.33 证明，若 $f(x)=x^p-x\in\mathbb{F}_p[x]$，则其多项式函数 $f^\flat:\mathbb{F}_p\to\mathbb{F}_p$ 恒为 0.

3.34 H (i) 若 p 是素数且 $m, n\in\mathbb{N}$，证明 $\binom{pm}{pn}\equiv\binom{m}{n}\bmod p$.

(ii) 证明 $\binom{p^rm}{p^rn}\equiv\binom{m}{n}\bmod p$ 对所有 $r\geqslant 0$ 成立.

(iii) 给出习题 1.72 的另一种证明：若 p 是素数且不整除整数 $m\geqslant 1$，则 $p\nmid\binom{p^rm}{p^r}$.

*3.35 设 $\alpha\in\mathbb{C}$，$\mathbb{Z}[\alpha]$ 是 $\mathbb{C}$ 的包含 α 的最小子环，即 $\mathbb{Z}[\alpha]=\bigcap S$，其中 S 取遍 $\mathbb{C}$ 的包含 α 的所有子环. 证明

$$\mathbb{Z}[\alpha]=\{f(\alpha): f(x)\in\mathbb{Z}[x]\}.$$

H 3.36 设 R 是交换环，$f(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$ 的次数 $n\geqslant 1$，定义它的导数 $f'(x)\in R[x]$ 为

$$f'(x)=a_1+2a_2x+3a_3x^2+\cdots+na_nx^{n-1};$$

若 $f(x)$ 是常数多项式，则定义它的导数是零多项式. 对于导数的这个定义，证明下列微积分法则是成立的：

$$(f+g)'=f'+g';$$
$$(rf)'=rf',\quad r\in R;$$
$$(fg)'=fg'+f'g;$$ 242

$$(f^n)' = nf^{n-1}f',\quad n \geqslant 1.$$

*3.37　假设在 $R[x]$ 中 $(x-a) \mid f(x)$. 证明，$R[x]$ 中 $(x-a)^2 \mid f(x)$ 当且仅当 $(x-a) \mid f'$.

3.38　(i)设 $f(x)=ax^{2p}+bx^p+c\in \mathbb{F}_p[x]$，证明 $f'(x)=0$.

H (ii)给出多项式 $f(x)\in \mathbb{F}_p[x]$ 的导数 $f'(x)=0$ 的充分必要条件，并加以证明.

*3.39　若 R 是一个交换环，则定义 $R[[x]]$ 为 R 上所有形式幂级数构成的集合.

H (i)证明 $R[x]$ 中定义的加法和乘法公式对 $R[[x]]$ 也有意义，并证明 $R[[x]]$ 对这些运算作成一个交换环.

(ii)证明 $R[x]$ 是 $R[[x]]$ 的一个子环.

(iii)记形式幂级数 $\sigma=(s_0, s_1, s_2, \cdots, s_n, \cdots)$ 为

$$\sigma = s_0 + s_1x + s_2x^2 + \cdots.$$

证明，若 $\sigma=1+x+x^2+\cdots$，则 $\sigma=1/(1-x)\in R[[x]]$.

*3.40　若 $\sigma=(s_0, s_1, s_2, \cdots, s_n, \cdots)$ 是一个非零形式幂级数，定义 $\mathrm{ord}(\sigma)=m$，其中 m 是满足 $s_m\neq 0$ 的最小自然数. 注意到 $\sigma\neq 0$ 当且仅当 $\mathrm{ord}(\sigma)$ 存在.

H (i)证明，若 R 是一个整环，则 $R[[x]]$ 是一个整环.

(ii)证明，若 k 是一个域，则非零形式幂级数 $\sigma\in k[[x]]$ 是单位当且仅当 $\mathrm{ord}(\sigma)=0$，即它的常数项不为零.

(iii)证明，若 $\sigma\in k[[x]]$ 且 $\mathrm{ord}(\sigma)=n$，则

$$\sigma = x^n u,$$

其中 u 是 $k[[x]]$ 中的单位.

→3.4　同态

正如我们可以利用同态比较群一样，我们也可以利用同态比较交换环.

→　**定义**　设 A 和 R 是交换环，则一个**(环)同态**是指一个函数 $f: A\to R$ 满足

(i) $f(1)=1$;

(ii)对所有 $a, a'\in A$，$f(a+a')=f(a)+f(a')$;

(iii)对所有 $a, a'\in A$，$f(aa')=f(a)f(a')$.

若一个同态同时也是双射，则称为**同构**. 若存在一个同构 $f: A\to R$，则交换环 A 和 R 称

243 为是**同构的**，记为 $A\cong R$.

→　**例 3.31**　(i)设 R 是一个整环，用 $F=\mathrm{Frac}(R)$ 表示它的分式域. 在定理 3.21 中我们说过，R 是 F 的一个子环，但这不是事实，R 甚至不是 F 的子集. 但是我们确实找到了 F 的一个子环 R'，它与 R 极其相似，即 $R'=\{[a, 1]: a\in R\}\subseteq F$. 容易看出，由 $f(a)=[a, 1]$ 给定的函数 $f: R\to R'$ 是一个同构. 今后，若我们证明了这一点，则把整环 R 看作 $\mathrm{Frac}(R)$ 的子环.

(ii)当把元素 $r\in R$ 和常数多项式 $(r, 0, 0, \cdots)$ 看作是相同时[见引理 3.26(iii)]，我们暗示了交换环 R 是 $R[x]$ 的一个子环. 我们知道 $R'=\{(r, 0, 0, \cdots): r\in R\}$ 是 $R[x]$ 的一个子环，并且易见由 $f(r)=(r, 0, 0, \cdots)$ 给定的函数 $f: R\to R'$ 是一个同构. ◀

例 3.32　(i)复共轭 $f: \mathbb{C}\to\mathbb{C}$，$z=a+ib\mapsto \bar{z}=a-ib$ 是一个同构，这是因为 $\bar{1}=1$，$\overline{z+w}=\bar{z}+\bar{w}$，$\overline{zw}=\bar{z}\bar{w}$. 由公式 $\bar{\bar{z}}=z$ 知复共轭是一个同构，这是因为复共轭的反函数是自身.

(ii)这里给出环同态不为同构的两个例子．若 R 是一个交换环，则(包含)同态 $f: R\to R[x]$不是满射(它是单射)．若 $m\geqslant 2$，则由 $f(n)=[n]$给定的映射 $f: \mathbb{Z}\to \mathbb{I}_m$ 不是单射(它是满射)．

(iii)前面的例子可以被推广．若 R 是一个交换环，其单位元记为 1，则由 $\chi(n)=n\cdot 1$ 给定的函数 $\chi: \mathbb{Z}\to R$ 是一个环同态． ◀

定理 3.33 设 R 和 S 是交换环，$\varphi: R\to S$ 是一个同态．若 $s_1,\cdots,s_n\in S$，则存在唯一一个同态

$$\tilde{\varphi}: R[x_1,\cdots,x_n]\to S$$

满足对所有 i 有$\tilde{\varphi}(x_i)=s_i$ 且对所有 $r\in R$ 有$\tilde{\varphi}(r)=\varphi(r)$．

证明 对 $n\geqslant 1$ 用归纳法证明．当 $n=1$ 时，记 x_1 为 x，记 s_1 为 s．定义$\tilde{\varphi}: R[x]\to S$ 如下：若 $f(x)=\sum_i r_i x^i$，则

$$\tilde{\varphi}: r_0+r_1x+\cdots+r_nx^n\mapsto \varphi(r_0)+\varphi(r_1)s+\cdots+\varphi(r_n)s^n=\tilde{\varphi}(f).$$

该公式表明$\tilde{\varphi}(x)=s$ 且对所有 $r\in R$ 有$\tilde{\varphi}(r)=\varphi(r)$． 244

现在只需证明$\tilde{\varphi}$是一个同态．首先，$\tilde{\varphi}(1)=\varphi(1)=1$，这是因为 φ 是一个同态．其次，若 $g(x)=a_0+a_1x+\cdots+a_mx^m$，则

$$\begin{aligned}\tilde{\varphi}(f+g)&=\tilde{\varphi}\Big(\sum_i(r_i+a_i)x^i\Big)\\&=\sum_i\varphi(r_i+a_i)s^i\\&=\sum_i(\varphi(r_i)+\varphi(a_i))s^i\\&=\sum_i\varphi(r_i)s^i+\sum_i\varphi(a_i)s^i\\&=\tilde{\varphi}(f)+\tilde{\varphi}(g).\end{aligned}$$

接着，令 $f(x)g(x)=\sum_k c_kx^k$，其中 $c_k=\sum_{i+j=k}r_ia_j$．则

$$\begin{aligned}\tilde{\varphi}(fg)&=\tilde{\varphi}\Big(\sum_k c_kx^k\Big)\\&=\sum_k\varphi(c_k)s^k\\&=\sum_k\varphi\Big(\sum_{i+j=k}r_ia_j\Big)s^k\\&=\sum_k\Big(\sum_{i+j=k}\varphi(r_i)\varphi(a_j)\Big)s^k.\end{aligned}$$

另一方面

$$\tilde{\varphi}(f)\,\tilde{\varphi}(g)=\Big(\sum_i\varphi(r_i)s^i\Big)\Big(\sum_j\varphi(a_j)s^j\Big)$$

$$= \sum_k \Big(\sum_{i+j=k} \varphi(r_i)\varphi(a_j) \Big) s^k.$$

我们用归纳法证明$\tilde{\varphi}$的唯一性. 先对 $d \geqslant 0$ 用归纳法证明基础步骤：若 $\theta: R[x] \to S$ 是一个同态，满足 $\theta(x)=s$ 且对所有 $r \in R$ 有 $\theta(r)=\varphi(r)$，则

$$\theta(r_0 + r_x + \cdots + r_d x^d) = \varphi(r_0) + \varphi(r_1)s + \cdots + \varphi(r_d)s^d.$$

对于归纳步骤，我们需要找到一个同态$\tilde{\varphi}$: $R[x_1, \cdots, x_{n+1}] \to S$，满足对所有 $i \leqslant n+1$ 有 $\tilde{\varphi}(x_i)=s_i$ 且对所有 $r \in R$ 有$\tilde{\varphi}(r)=\varphi(r)$. 若我们定义 $A=R[x_1, \cdots, x_n]$，则归纳假设给出一个同态 $\psi: A \to S$，满足对所有 $i \leqslant n$ 有 $\psi(x_i)=s_i$ 且对所有 $r \in R$ 有 $\psi(r)=\varphi(r)$. 基础步骤给出
245 一个同态$\tilde{\psi}$: $A[x_{n+1}] \to S$，满足$\tilde{\psi}(x_{n+1})=s_{n+1}$且对所有 $a \in A$ 有$\tilde{\psi}(a)=\psi(a)$. 最终结论源于以下事实：$R[x_1, \cdots, x_{n+1}]=A[x_{n+1}]$，对所有 $i \leqslant n$ 有$\tilde{\psi}(x_i)=\psi(x_i)=s_i$，$\tilde{\psi}(x_{n+1})=\psi(x_{n+1})=s_{n+1}$，对所有 $r \in R$ 有$\tilde{\psi}(r)=\psi(r)=\varphi(r)$. ■

→ **定义** 若 R 是交换环，$a \in R$，则**赋值** a 是指函数 $e_a: R[x] \to R$，$e_a(f(x))=f(a)$，即

$$e_a\Big(\sum_i r_i x^i\Big) = \sum_i r_i a^i.$$

→ **推论 3.34** 若 R 是交换环，$a \in R$，则赋值映射 $e_a: R[x] \to R$ 是一个同态.

证明 在定理 3.33 中，设 $R=S$ 和 $\varphi=1_R$，则$\tilde{\varphi}=e_a$. ■

环同态 $f: A \to R$ 的一些性质是根据它是加法群 A 和 R 之间的群同态得到的. 例如，$f(0)=0$，$f(-a)=-f(a)$，$f(na)=nf(a)$，所有 $n \in \mathbb{Z}$. 对于不熟悉群的读者，我们证明这些结论. 因为 $0+0=0$，所以 $f(0)=f(0)+f(0)$，两边减去 $f(0)$得 $f(0)=0$. 因为$-a+a=0$，所以 $f(-a)+f(a)=f(0)=0$，两边减去 $f(a)$得 $f(-a)=-f(a)$. 对 $n \geqslant 0$ 用归纳法证明：对所有 $n \geqslant 0$ 和所有 $a \in R$ 有 $f(na)=nf(a)$. 最后，若 $n<0$，则用$-a$ 代替 a 得到结论. 同态保持乘法有一个类似结论.

引理 3.35 若 $f: A \to R$ 是一个环同态，则对所有 $a \in A$，

(i) 对所有 $n \geqslant 0$ 有 $f(a^n)=f(a)^n$；

(ii) 若 a 是一个单位，则 $f(a)$也是一个单位，且 $f(a^{-1})=f(a)^{-1}$；

(iii) 若 a 是一个单位，则对所有 $n \geqslant 1$ 有 $f(a^{-n})=f(a)^{-n}$.

证明 (i) 若 $n=0$，则 $f(a^0)=1=(f(a))^0$，这是因为每个环同态都满足 $r^0=1$ 和$f(1)=1$，r 为环的任意元素. 对正整数 $n \geqslant 1$ 用归纳法可证明命题成立.

(ii) 用 f 作用等式 $a^{-1}a=1$，可证明 $f(a)$是一个单位，其逆元为 $f(a^{-1})$.

(iii) 回忆 $a^{-n}=(a^{-1})^n$，并利用(i)和(ii)可证得. ■

推论 3.36 若 $f: A \to R$ 是一个环同态，则

$$f(U(A)) \subseteq U(R),$$

其中 $U(A)$是由 A 的单位构成的群. 若 f 是一个同构，则存在一个群同构

246 $$U(A) \cong U(R).$$

证明 第一个命题只是引理 3.35(ii)的一个重述：若 a 是 A 的一个单位，则 $f(a)$是 R 的一个单位.

若 f 是一个同构，则根据习题 3.44(i)知它的反函数 $f^{-1}: R \to A$ 也是一个环同态．因而，若 r 是 R 的一个单位，则 $f^{-1}(r)$ 是 A 的一个单位．现在容易检验 $\varphi: U(A) \to U(R)$，$a \mapsto f(a)$ 是一个(群)同构，这是因为它的反函数是 $\psi: U(R) \to U(A)$，$r \mapsto f^{-1}(r)$． ■

例 3.37　若 X 是非空集合，定义 X 上的**位串**为函数 $\beta: X \to \mathbb{F}_2$，$X$ 上的所有位串构成的集合记为 $b(X)$．若 X 是有限的，不妨设 $X=\{x_1, \cdots, x_n\}$，则位串是由 0 和 1 组成的长度为 n 的序列．

在 $b(X)$ 上定义二元运算：设 β，$\gamma \in b(X)$，定义

$$\beta\gamma: x \mapsto \beta(x)\gamma(x)$$

和

$$\beta+\gamma: x \mapsto \beta(x)+\gamma(x).$$

$b(X)$ 在这些运算下是一个交换环，这是习题 3.10 中 $R=\mathbb{F}_2$ 时的特殊情形．

回忆布尔环 $\mathcal{B}(X)$［见习题 3.7(i)］，其元素是 X 的子集，其乘法运算定义为交：$AB=A\cap B$，其加法运算定义为对称差：$A+B=(A-B)\cup(B-A)$．我们现在证明 $\mathcal{B}(X)\cong b(X)$．

若 A 是集合 X 的子集，则定义它的**特征函数**为 $\chi_A: X \to \mathbb{F}_2$，

$$\chi_A(x)=\begin{cases}1 & \text{当 } x\in A\\ 0 & \text{当 } x\notin A.\end{cases}$$

例如，$\chi_\varnothing$ 是常数函数 $\chi_\varnothing(x)=0$，任意 $x\in X$．χ_X 是常数函数 $\chi_X(x)=1$，任意 $x\in X$．

定义 $\varphi: \mathcal{B}(X) \to b(X)$，$\varphi(A)=\chi_A$．若 $x\in X$，则 $x\in A$ 当且仅当 $\chi_A(x)=1$．因此，若 $\chi_A=\chi_B$，则 $x\in A$ 当且仅当 $x\in B$，即 $A=B$．于是 φ 是单射．实际上，φ 是一个双射，这是因为：若 $f: X\to\mathbb{F}_2$ 是一个位串，则 $\varphi(A)=f$，其中 $A=\{x\in X: f(x)=1\}$．

我们现在证明 φ 是一个环同构．$\mathcal{B}(X)$ 中的单位元是 X，并且 $\varphi(X)=\chi_X$ 是取值为 1 的常数函数，它是 $b(X)$ 中的单位元．设 A 和 B 是 X 的子集．若 $x\in X$，则

$$(\chi_A\chi_B)(x)=1 \quad \text{当且仅当} \quad x\in A \text{ 且 } x\in B;$$

即 $\chi_A\chi_B=\chi_{A\cap B}$．因此 $\varphi(AB)=\varphi(A)\varphi(B)$．另外，

$$(\chi_A+\chi_B)(x)=1 \quad \text{当且仅当} \quad x\in A \text{ 和 } x\in B \text{ 有且仅有一个成立,}$$ 247

即 $\chi_A+\chi_B=\chi_{(A\cup B)-(A\cap B)}=\chi_{A+B}$［回忆习题 2.4：$A+B=(A\cup B)-(A\cap B)$］．因此 $\varphi(A+B)=\varphi(A)+\varphi(B)$．这样 φ 是一个同构． ◀

→　**定义**　*若 $f: A\to R$ 是一个环同态，则它的核是*

$$\ker f=\{a\in A: f(a)=0\},$$

它的象是

$$\operatorname{im} f=\{r\in R: \text{存在 } a\in A \text{ 可使 } r=f(a)\}.$$

注意，若我们不考虑乘法，则环 A 和 R 都是加法阿贝尔群，并且这些定义与群论中的定义相一致．

设 k 是一个域，$a\in k$，和推论 3.34 一样，考虑赋值同态 $e_a: k[x]\to k$，$f(x)\mapsto f(a)$．现在 e_a 总是满射，这是因为若 $b\in k$ 则 $b=e_a(f)$，其中 $f(x)=x-a+b$．这样 $\operatorname{im} e_a=k$．根据定

义，$\ker e_a$ 由所有满足 $g(a)=0$ 的多项式 $g(x)$ 构成，即 $\ker e_a$ 由 $k[x]$中所有具有根 a 的多项式构成.

命题 3.38 设 $f: A\to R$ 是一个环同态，其中 R 是非零环，则 $\mathrm{im} f$ 是 R 的子环，$\ker f$ 是 A 的真子集且满足下列结论：

(i)$0\in\ker f$;

(ii)若 x，$y\in\ker f$，则 $x+y\in\ker f$;

(iii)若 $x\in\ker f$，$a\in A$，则 $ax\in\ker f$.

证明 若 r，$r'\in\mathrm{im} f$，则存在 a，$a'\in A$ 使得 $r=f(a)$，$r'=f(a')$. 因此，$r-r'=f(a)-f(a')=f(a-a')\in\mathrm{im} f$，$rr'=f(a)f(a')=f(aa')\in\mathrm{im} f$. 由同态的定义知 $f(1)=1$，因此 $\mathrm{im} f$ 是 R 的子环.

因为 $f(0)=0$，所以 $0\in\ker f$. 若 x，$y\in\ker f$，则 $f(x+y)=f(x)+f(y)=0+0=0$，因此 $x+y\in\ker f$. 若 $x\in\ker f$，$a\in A$，则 $f(ax)=f(a)f(x)=f(a)0=0$，因此 $ax\in\ker f$. 因为 $f(1)=1\neq 0$，所以 $1\notin\ker f$，因此 $\ker f$ 是 A 的真子集. ■

群同态 $G\to H$ 的核不仅是子群还是正规子群：它在结合运算下关于群 G 的元素与它自身的元素是封闭的. 类似地，若 $f: A\to R$ 是一个环同态，则 $\ker f$ 几乎[⊖]是一个子环：它在加法和乘法运算下是封闭的. 另外 $\ker f$ 在乘法运算下关于交换环 A 的元素与 $\ker f$ 的元素是封
248 闭的.

→ **定义** 交换环 R 的子集 I 称为 R 中的**理想**是指 I 满足下列条件：

(i)$0\in I$;

(ii)若 a，$b\in I$，则 $a+b\in I$;

(iii)若 $a\in I$，$r\in R$，则 $ra\in I$.

理想 $I\neq R$ 称为**真理想**.

命题 3.38 可以被重述如下：若 $f: A\to R$ 是一个环同态，其中 R 是非零环，则 $\mathrm{im} f$ 是 R 的子环而 $\ker f$ 是 A 中的真理想.

在任何非零交换环 R 中总存在两个理想：环 R 本身和仅由 0 构成的子集$\{0\}$. 在命题 3.43 中我们将看到：若交换环只有这两个理想，则它是域.

→ **例 3.39** 若 b_1，b_2，…，b_n 是交换环 R 中的元素，则它们的所有线性组合构成的集合

$$I=\{r_1b_1+r_2b_2+\cdots+r_nb_n: \text{对所有 } i, r_i\in R\}$$

是 R 中的一个理想. 此时我们记 $I=(b_1, b_2, \cdots, b_n)$. 特别地，若 $n=1$，则

$$I=(b)=\{rb: r\in R\}$$

是 R 中的一个理想，它是由 b 的所有倍数所构成的，称之为由 b 生成的**主理想**.

注意，R 和$\{0\}$恒为主理想：$R=(1)$，$\{0\}=(0)$. 在$\mathbb{Z}$ 中，偶数构成主理想(2). ◀

→ **定理 3.40** $\mathbb{Z}$ 中的每个理想都是主理想.

⊖ 若 $f: A\to R$ 且 A，R 均是非零环，则 $\ker f$ 不是子环，这是因为它不包含 1：若 1 是 A 的单位元，则 $1\neq 0$，$f(1)=1\neq 0$.

证明 这仅仅是推论 1.37 的重新叙述. ■

两个元素能否生成相同的主理想?

命题 3.41 *若 R 是交换环且存在单位 $u\in R$ 使得 $a=ub$，则 $(a)=(b)$. 反之，若 R 是整环且 $(a)=(b)$，则存在单位 $u\in R$ 使得 $a=ub$.*

证明 假设存在单位 $u\in R$ 使得 $a=ub$. 若 $x\in(a)$，则存在 $r\in R$ 使得 $x=ra=rub\in(b)$，因此 $(a)\subseteq(b)$. 对于反包含，若 $y\in(b)$，则存在 $s\in R$ 使得 $y=sb=su^{-1}a\in(a)$，因此 $(b)\subseteq(a)$. 这样 $(a)=(b)$.

反之，若 $(a)=(b)$，则 $a\in(a)=(b)$，因此存在 $r\in R$ 使得 $a=rb$，也就是说，$b\mid a$. 类似的，由 $b\in(b)=(a)$ 可推出 $a\mid b$. 因为 R 是整环，所以由命题 3.15 知存在单位 $u\in R$ 使得 $a=ub$. ■ 249

例 3.42 若交换环 R 中的理想 I 含有 1，则 $I=R$，这是因为此时 I 含有 $r=r1$，$\forall r\in R$. 事实上，一个理想 I 含有单位 u 当且仅当 $I=R$. 充分性是显然的：若 $I=R$，则 I 含有单位 1. 反之，若存在单位 $u\in I$，则 I 含有 $u^{-1}u=1$，于是 I 含有 $r=r1$，$\forall r\in R$. ◀

→ **命题 3.43** *非零交换环 R 是域当且仅当 R 中的理想只有 $\{0\}$ 和 R 本身.*

证明 假设 R 是域. 若 $I\neq\{0\}$，则 I 含有某个非零元，而域中的每个非零元都是单位. 因此，由例 3.42 知 $I=R$.

反之，假设 R 是交换环，其理想只有 R 和 $\{0\}$. 若 $a\in R$ 且 $a\neq0$，则主理想 $(a)\neq0$，从而 $(a)=R$，所以 $1\in R=(a)$. 因此存在 $r\in R$ 使 $1=ra$，即 a 在 R 中有逆元，所以 R 是一个域. ■

命题 3.44 *环同态 $f: A\to R$ 是单射当且仅当 $\ker f=\{0\}$.*

证明 假设 f 是单射，若 $a\neq 0$ 则 $f(a)\neq f(0)=0$，这样 $a\notin\ker f$，因此 $\ker f=\{0\}$. 反之，假设 $\ker f=\{0\}$，令 $f(a)=f(a')$，则 $0=f(a)-f(a')=f(a-a')$，因此 $a-a'\in\ker f=\{0\}$，这样 $a=a'$，即 f 是单射.（读者可以验证当 A 或 R 是零环时该命题也成立.） ■

推论 3.45 *若 $f: k\to R$ 是一个环同态，其中 R 是非零环，k 是域，则 f 是一个单射.*

证明 根据上面命题，只须证明 $\ker f=\{0\}$. 但由命题 3.38 知，$\ker f$ 是 k 中的真理想，而命题 3.43 表明 k 只有两个理想 k 和 $\{0\}$. 因为 $f(1)=1\neq0$(R 是非零环)，所以 $\ker f\neq k$，因此 $\ker f=\{0\}$，这样 f 是单射. ■

习题

H 3.41 判断对错并说明理由.

(i) 若 R 和 S 都是交换环，$f: R\to S$ 是一个环同态，则 f 也是 R 的加法群到 S 的加法群的一个同态.

(ii) 若 R 和 S 都是交换环，f 是 R 的加法群到 S 的加法群的一个同态，且满足 $f(1)=1$，则 f 是一个环同态. 250

(iii) 若 R 和 S 是同构的交换环，则任意环同态 $f: R\to S$ 是一个同构.

(iv) 若 $f: R\to S$ 是一个环同态，其中 S 是非零环，则 $\ker f$ 是 R 中的一个真理想.

(v) 若 I 和 J 都是交换环 R 中的理想，则 $I\cap J$ 和 $I\cup J$ 也是 R 中的理想.

(vi) 若 $\varphi: R\to S$ 是一个环同态，I 是 R 的中一个理想，则 $\varphi(I)$ 是 S 中的一个理想.

(vii) 若 $\varphi: R\to S$ 是一个环同态，J 是 S 中的一个理想，则逆象 $\varphi^{-1}(J)$ 是 R 中的一个理想.

(viii)若 R 和 S 都是交换环，则投射$(r, s)\mapsto r$是环同态$R\times S\to R$.

(ix)若 k 是一个域，$f: k\to R$ 是一个满环同态，则 R 是一个域.

(x)若 $f(x)=e^x$，则 f 是$\mathcal{F}(\mathbb{R})$中的单位.

3.42 设 A 是一个交换环. 证明 A 的子集 J 是一个理想当且仅当 $0\in J$，由 $u, v\in J$ 可推出 $u-v\in J$，由 $u\in J$，$a\in A$ 可推出 $au\in J$.（为了使 J 是一个理想，由 $u, v\in J$ 应推出 $u+v\in J$，而不是 $u-v\in J$.）

3.43 (i)证明只含 4 个元素的域 F(见习题 3.19)是与$\mathbb{I}_4$ 不同构的交换环.

H (ii)证明任意两个只含有 4 个元素的域是同构的.

*3.44 (i)设 $\varphi: A\to R$ 是一个同构，$\psi: R\to A$ 是它的反函数. 证明 ψ 是一个同构.

(ii)证明两个同态(或两个同构)的合成也是一个同态(或一个同构).

(iii)证明 $A\cong R$ 定义了任一族交换环上的一个等价关系.

3.45 设 R 是一个交换环，$\mathcal{F}(R)$是所有函数 $f: R\to R$ 构成的交换环(看习题 3.10).

(i)证明，R 与$\mathcal{F}(R)$的由所有常数函数构成的子环同构.

(ii)若 $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$，设 $f^\flat: R\to R$，$f^\flat(r)=a_0+a_1r+\cdots+a_nr^n$[因此，$f^\flat$是与 $f(x)$相联系的多项式函数]. 证明由 $\varphi: f(x)\mapsto f^\flat$定义的函数 $\varphi: R[x]\to\mathcal{F}(R)$是一个环同态.

(iii)证明，若 $R=\mathbf{F}_p$，其中 p 是一个素数，则 $x^p-x\in\ker\varphi$.（我们将在定理 3.50 中证明，当 R 是一个无限域时，φ 是单射.）

3.46 设 R 是一个交换环，证明函数 $\eta: R[x]\to R$，

$$\eta: a_0+a_1x+a_2x^2+\cdots+a_nx^n\mapsto a_0,$$

是一个同态. 用多项式的根描述 $\ker\eta$.

*3.47 设 $\psi: R\to S$ 是一个同态，其中 R 和 S 都是交换环，且 $\ker\psi=I$. 若 J 是 S 中的一个理想，证明 $\psi^{-1}(J)$ 是 R 中的包含 I 的一个理想.

H 3.48 若 R 是一个交换环且 $c\in R$，证明函数 $\varphi: R[x]\to R[x]$，$f(x)\mapsto f(x+c)$是一个同构. 详细地说，

251 $$\varphi\Big(\sum_i s_ix^i\Big)=\sum_i s_i(x+c)^i.$$

3.49 若 R 是一个域，证明 $R\cong\mathrm{Frac}(R)$. 准确地说，证明例 3.31 中的同态 $f: R\to\mathrm{Frac}(R)$，$r\mapsto[r, 1]$是一个同构.

*3.50 设 R 是一个整环，F 是包含子环 R 的一个域.

(i)证明 $E=\{uv^{-1}: u, v\in R, v\neq 0\}$是 F 的包含子环 R 的一个子域.

(ii)证明 $\mathrm{Frac}(R)\cong E$，其中 E 是(i)中定义的 F 的子域.（参见习题 3.23.）

*3.51 H (i)若 A，R 都是整环，$\varphi: A\to R$ 是一个环同构，则$[a, b]\mapsto[\varphi(a), \varphi(b)]$是环同构 $\mathrm{Frac}(A)\to\mathrm{Frac}(R)$.

(ii)证明，若域 k 含有与$\mathbb{Z}$同构的子环，则 k 一定含有与$\mathbb{Q}$同构的子域.

3.52 设 R 是一个整环，其分式域 $F=\mathrm{Frac}(R)$.

(i)证明 $\mathrm{Frac}(R[x])\cong F(x)$.

(ii)证明 $\mathrm{Frac}(R[x_1, x_2, \cdots, x_n])\cong F(x_1, x_2, \cdots, x_n)$.

3.53 (i)若 R，S 都是交换环，证明它们的直积 $R\times S$ 也是一个交换环，其中 $R\times S$ 中的加法和乘法定义为

$$(r,s)+(r',s')=(r+r',s+s'),\quad (r,s)(r',s')=(rr',ss').$$

(ii)证明 $R\times\{0\}$是 $R\times S$ 的一个理想.

(iii)证明，若 R 和 S 都不是零环，则 $R\times S$ 不是一个整环.

*3.54 H (i)若 R，S 都是交换环，证明

$$U(R\times S)=U(R)\times U(S),$$

其中 $U(R)$ 是 R 的单位构成的群.

H (ii)证明，若 m 和 n 是互素的整数，则作为环 $\mathbb{I}_{mn}\cong\mathbb{I}_m\times\mathbb{I}_n$.

(iii)利用(ii)给出推论 2.131 的另一个证明：若 $(m,n)=1$，则 $\phi(mn)=\phi(m)\phi(n)$，其中 ϕ 是欧拉 ϕ-函数.

3.55 (i)设 F 是形如 $A=\begin{bmatrix} a & b \\ -b & a\end{bmatrix}$ 的所有 2×2 实矩阵构成的集合，证明 F 对矩阵加法和矩阵乘法作成一个域.

H (ii)证明 F 与 $\mathbb{C}$ 同构.

→3.5 从数到多项式

我们将会看到，当 k 是域时，第 1 章中关于 $\mathbb{Z}$ 的所有定理实际上在 $k[x]$ 中都有关于多项式的类似结论，而且还会看到那些证明可以改写成这里的证明.

系数在域中的多项式的除法算式是说，长除法是可能的.

$$s_nx^n+s_{n-1}x^{n-1}+\cdots \;\overline{\big)\, t_mx^m+t_{m-1}x^{m-1}+\cdots}^{\;s_n^{-1}t_mx^{m-n}+\cdots}$$ 252

→ **定义** 若 $f(x)=s_nx^n+\cdots+s_1x+s_0$ 是 n 次多项式，则它的首项是

$$\mathrm{LT}(f)=s_nx^n.$$

回忆 $f(x)$ 的首项系数是 s_n.

设 k 是域，令 $f(x)=s_nx^n+\cdots+s_1x+s_0$ 和 $g(x)=t_mx^m+\cdots+t_1x+t_0$ 是 $k[x]$ 中的多项式，满足 $\deg(f)\leqslant\deg(g)$，即 $n\leqslant m$. 因为 k 是域，所以 $s_n^{-1}\in k$，且

$$\frac{\mathrm{LT}(g)}{\mathrm{LT}(f)}=s_n^{-1}t_mx^{m-n}\in k[x];$$

因此 $\mathrm{LT}(f)\mid\mathrm{LT}(g)$. 更一般地，设 k 是任意交换环，若 s_n 是 k 中的一个单位，则在 $k[x]$ 中有 $\mathrm{LT}(f)\mid\mathrm{LT}(g)$.

→ **定理 3.46(除法算式)** 假设 R 是一个交换环，且 $f(x)$，$g(x)\in R[x]$，$f(x)$ 的首项系数是 R 中的单位.

(i)存在多项式 $q(x)$，$r(x)\in R[x]$ 满足

$$g(x)=q(x)f(x)+r(x),$$

其中 $r(x)=0$ 或 $\deg(r)<\deg(f)$.

(ii)若 R 是一个整环，则(i)中的多项式 $q(x)$ 和 $r(x)$ 是唯一的.

注 若 R 是一个域，则假设 $f(x)$ 的首项系数是一个单位如同假设 $f(x)\neq 0$.

证明 (i)我们先证明 $q(x)$，$r(x)\in R[x]$ 的存在性. 若 $f\mid g$，则存在某个 q 使得 $g=qf$，定义余项 $r=0$，定理得证. 若 $f\nmid g$，则当 q 在 $k[x]$ 中变化时，考虑所有形如 $g-qf$ 的多项式(一定不为零). 由最小数原理知存在一个次数最小的多项式 $r=g-qf$. 由于 $g=qf+r$，所以只须证明 $\deg(r)<\deg(f)$. 记 $f(x)=s_nx^n+\cdots+s_1x+s_0$ 和 $r(x)=t_mx^m+\cdots+t_1x+t_0$. 由题设知 s_n 是一个单位，因此 $s_n^{-1}\in k$. 假设 $\deg(r)\geqslant\deg(f)$，则定义 $h(x)$ 为

$$h(x)=r(x)-t_ms_n^{-1}x^{m-n}f(x);$$

即 $h=r-[LT(r)/LT(f)]f$，注意 $h=0$ 或 $\deg(h)<\deg(r)$．若 $h=0$，则 $r=[\mathrm{LT}(r)/\mathrm{LT}(f)]f$ 且

253

$$g = qf + r = qf + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}f = \left[q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}\right]f,$$

此与 $f\nmid g$ 矛盾．若 $h\neq 0$，则 $\deg(h)<\deg(r)$ 且

$$g - qf = r = h + \frac{\mathrm{LT}(r)}{LT(f)}f.$$

因此 $g-[q+\mathrm{LT}(r)/\mathrm{LT}(f)]f=h$，此又与 r 是这种形式的多项式中次数最小的多项式相矛盾．因此，$\deg(r)<\deg(f)$．

(ii)为证明 $q(x)$ 和 $r(x)$ 的唯一性，假设 $g=q'f+r'$，其中 $\deg(r')<\deg(f)$．则

$$(q-q')f = r' - r.$$

若 $r'\neq r$，则每一边都有次数．但 $\deg((q-q')f)=\deg(q-q')+\deg(f)\geqslant\deg(f)$，而 $\deg(r'-r)\leqslant\max\{\deg(r'),\deg(r)\}<\deg(f)$，矛盾．因而 $r'=r$，$(q-q')f=0$．因为 R 是整环，所以 $R[x]$ 也是整环．于是 $q-q'=0$，$q=q'$． ■

我们给出的关于多项式的除法算式的证明是一个间接的证明，但这个证明可以被重算使得它是一个真正的算式，这与关于整数的除法算式一样．下面是实施它的一个伪码．

```
Input: g, f
Output: q, r
q := 0;    r := g
WHILE  r≠0  AND  LT(f) | LT(r)  DO
  q := q+[LT(r)/LT(f)]x^(deg(r)-deg(f))
  r := r-[LT(q)/LT(f)]f
END  WHILE
```

→ **定义** 若 $f(x)$，$g(x)$ 都是 $k[x]$ 中的多项式，其中 k 是域，则除法算式中的多项式 $q(x)$ 和 $r(x)$ 称为用 $f(x)$ 除 $g(x)$ 后的**商式**和**余式**．

下面的定理在 $\mathbb{Z}[x]$ 中利用除法算式用首一多项式去除．回忆前面定义的分圆多项式．

定理 3.47 对每个正整数 n，分圆多项式 $\Phi_n(x)$ 都是一个带整系数的首一多项式．

证明 对 $n\geqslant 1$ 用归纳法证明．基础步骤是成立的，因为 $\Phi_1(x)=x-1$．对于归纳步，我们假设 $\Phi_d(x)$ 是一个带整系数的首一多项式．根据等式 $x^n-1=\prod_d\Phi_d(x)$（见命题 1.30），我们有

254

$$x^n - 1 = \Phi_n(x)f(x),$$

其中 $f(x)$ 是所有 $\Phi_d(x)$ 的乘积，其中 d 是 n 的真因子（即 $d\mid n$ 且 $d<n$）．根据归纳假设，$f(x)$ 是一个带整系数的首一多项式．因为 $f(x)$ 是首一的，所以由 $\mathbb{Z}[x]$ 中关于首一多项式的除法算式知 $(x^n-1)/f(x)\in\mathbb{Z}[x]$，因此 $\Phi_n(x)=(x^n-1)/f(x)$ 的所有系数都是整数． ■

我们现在把注意力转到多项式的根上来．

→ **定义** 若 $f(x)\in k[x]$，其中 k 是域，则 $f(x)$ 在 k 中的**根**是指元素 $a\in k$ 满足 $f(a)=0$．

注 多项式 $f(x)=x^2-2$ 的系数在 $\mathbb{Q}$ 中，尽管 $\sqrt{2}\notin\mathbb{Q}$，但我们通常说 $\sqrt{2}$ 是 $f(x)$ 的一

个根．我们将在定理 3.118 中看到：对每个多项式 $f(x)\in k[x]$，其中 k 是任意域，都存在一个更大的域 E，它包含 k 作为子域且含有 $f(x)$ 的所有的根． ◀

引理 3.48 设 $f(x)\in k[x]$，其中 k 是域，并设 $a\in k$．则存在 $q(x)\in k[x]$ 满足

$$f(x)=q(x)(x-a)+f(a).$$

证明 利用除法算式得

$$f(x)=q(x)(x-a)+r,$$

因为 $x-a$ 的次数为 1，所以余式 r 是一个常数．根据推论 3.34，赋值 a 是一个环同态 e_a：$k[x]\to k$：

$$e_a(f)=e_a(q)e_a(x-a)+e_a(r).$$

因此，$f(a)=q(a)(a-a)+r$，$r=f(a)$． ■

根与因子之间存在某种联系．

命题 3.49 若 $f(x)\in k[x]$，其中 k 是域，则 $a\in k$ 是 $f(x)$ 在 k 中的一个根当且仅当在 $k[x]$ 中 $x-a$ 能整除 $f(x)$．

证明 若 a 是 $f(x)$ 在 k 中的一个根，则 $f(a)=0$，于是由引理 3.48 知 $f(x)=q(x)(x-a)$．反之，若 $f(x)=q(x)(x-a)$，则赋值 a（即应用 e_a）得 $f(a)=q(a)(a-a)=0$． ■

定理 3.50 若 k 是域，$f(x)\in k[x]$ 的次数为 n，则 $f(x)$ 在 k 中至多有 n 个根． 255

证明 对 $n\geq 0$ 用归纳法证明．若 $n=0$，则 $f(x)$ 是一个非零常数，这样 $f(x)$ 在 k 中根的个数为零．现设 $n>0$，若 $f(x)$ 在 k 内没有根，则证毕，因为 $0\leqslant n$．否则，我们可假设存在 $a\in k$ 使得 a 是 $f(x)$ 的一个根．因而，由命题 3.49 知

$$f(x)=q(x)(x-a),$$

且 $q(x)\in k[x]$ 的次数为 $n-1$．若存在一个根 $b\in k$ 满足 $b\neq a$，则

$$0=f(b)=q(b)(b-a).$$

因为 $b-a\neq 0$，而 k 是域（因而是整环），所以 $q(b)=0$，所以 b 是 $q(x)$ 的一个根．现在 $\deg(q)=n-1$，由归纳假设知 $q(x)$ 在 k 中至多有 $n-1$ 个根．因此，$f(x)$ 在 k 中至多有 n 个根． ■

例 3.51 定理 3.50 对任意交换环不成立．多项式 $x^2-[1]\in \mathbb{I}_8[x]$ 在 $\mathbb{I}_8$ 中有 4 个不同的根，即 [1]，[3]，[5]，[7]． ◀

回忆一下，每个多项式 $f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_0\in k[x]$ 可确定一个多项式函数 $f^\flat$：$k\to k$，对所有 $a\in k$ 满足 $f^\flat(a)=c_na^n+c_{n-1}a^{n-1}+\cdots+c_0$．然而，在习题 3.33 中，我们看到 $\mathbf{F}_p[x]$ 中的非零多项式（例如 x^p-x）可以确定常数函数 0．当 k 是无限域时，这一病态会消失．

推论 3.52 设 k 是一个无限域，$f(x)$ 与 $g(x)$ 是 $k[x]$ 中的多项式．若 $f(x)$ 与 $g(x)$ 确定同一个多项式函数，即对所有 $a\in k$ 有 $f^\flat(a)=g^\flat(a)$，则 $f(x)=g(x)$．

证明 假设 $f(x)\neq g(x)$，则多项式 $f(x)-g(x)$ 不为零，所以它有某个次数，不妨设为 n．因为对所有 $a\in k$ 有 $f^\flat(a)=g^\flat(a)$，所以 k 的每个元素都是 $f(x)-g(x)$ 的根．k 是无限的，而由定理 3.50 知这个 n 次多项式至多有 n 个根，矛盾． ■

实际上，上述证明给出了更多的东西．

推论 3.53 设 k 是任意一个(可能有限)域，$f(x)$，$g(x)\in k[x]$，且 $n=\max\{\deg(f),\deg(g)\}$. 若存在 $n+1$ 个元素 $a\in k$ 可使 $f(a)=g(a)$，则 $f(x)=g(x)$.

证明 若 $f(x)\neq g(x)$，则 $h(x)=f(x)-g(x)\neq 0$，且

$$\deg(h)\leqslant \max\{\deg(f),\deg(g)\}=n.$$

根据题设，存在 $n+1$ 个元素 $a\in k$ 可使 $h(a)=f(a)-g(a)=0$，此与定理 3.50 矛盾. 因此
256 $h(x)=0$，$f(x)=g(x)$. ■

记号 若 a_1，a_2，…，a_n 是一个序列，则 a_1，…，$\hat{a}_i$，…，a_n 表示原序列去掉 a_i 后得到的子序列.

推论 3.54 (拉格朗日插值法) 设 k 是一个域，u_0，…，u_n 是 k 中不同元素. 给定 k 中任意序列 y_0，…，y_n，则存在唯一一个次数$\leqslant n$ 的多项式 $f(x)\in k[x]$满足 $f(u_i)=y_i$，其中 $i=0$，…，n. 实际上，

$$f(x)=\sum_{i=0}^{n}y_i\frac{(x-u_0)\cdots\widehat{(x-u_i)}\cdots(x-u_n)}{(u_i-u_0)\cdots\widehat{(u_i-u_i)}\cdots(u_i-u_n)}.$$

证明 公式中出现的多项式 $f(x)$的次数至多为 n，并且对所有 i 有 $f(u_i)=y_i$. 利用推论 3.53可证明唯一性. ■

注 利用习题 1.15，拉格朗日插值法可以被简化：若 $f=g_1\cdots g_n$，则 $f'=\sum_{i=1}^{n}d_if$，其中 $d_if=g_1\cdots g_i'\cdots g_n$. 若 $g_i(x)=x-u_i$，则 $d_if=(x-u_1)\cdots\widehat{(x-u_i)}\cdots(x-u_n)$. 因此

$$f(x)=\sum_{i=1}^{n}y_i\frac{d_if(x)}{d_if(u_i)}.$$

→ **定理 3.55** 若 k 是一个域，G 是乘法群 $k^{\times}$ 的一个有限子群，则 G 是一个循环群. 特别的，若 k 本身是有限的(例如 $k=\mathbf{F}_p$)，则 $k^{\times}$ 是一个循环群.

证明 设 d 是 $|G|$ 的一个因子. 若 G 有两个阶为 d 的子群 S 和 T，则 $|S\cup T|>d$. 对每个 $a\in S\cup T$ 有 $a^d=1$，因此它是 x^d-1 的根. x^d-1 在 k 中有太多的根，这与定理 3.50 矛盾. 这样，由命题 2.75 知 G 是一个循环群. ■

虽然乘法群$\mathbf{F}_p^{\times}$是循环群，但没有明确的公式可以给出它的生成元. 换句话说，设$[s(p)]$是$\mathbf{F}_p^{\times}$的生成元，但没有有效的算法用以计算 $s(p)$.

$k[x]$中最大公因子的定义本质上与整数最大公因子的定义一致，其中 k 是一个域. 不久我们将在一般整环中定义最大公因子的概念.

→ **定义** 若 k 是域，且 $f(x)$，$g(x)\in k[x]$，则**公因子**是指多项式 $c(x)\in k[x]$满足 $c(x)\mid f(x)$和 $c(x)\mid g(x)$.

若 $f(x)$，$g(x)$至少有一个非零，则它们的**最大公因子**[缩写为 gcd，记为(f,g)]定义为
257 它们的次数最大的那个首一公因子. 若 $f(x)=0=g(x)$，则它们的最大公因子定义为 0.

→ **命题 3.56** 设 k 是域，则每对 $f(x)$，$g(x)\in k[x]$都有最大公因子.

证明 当 $f(x)$和 $g(x)$都等于 0 时，结论显然成立. 我们假设 $f(x)\neq 0$. 若 $h(x)$是 $f(x)$

的一个因子，则 $\deg(h)\leqslant\deg(f)$，这样 $\deg(f)$是 $f(x)$和 $g(x)$的公因子的次数的上界．设 $d(x)$是次数最大的公因子，因为 k 是域，所以我们可以假设 $d(x)$是首一的[若 $d(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0$，则 $a_m^{-1}d(x)$是一个首一公因子，其次数为 $m=\deg(d)$]．因此 $d(x)$是**最大公因子**． ■

这里有一个类似于定理 1.35 的结论，我们将利用它去证明最大公因子的唯一性．

→ **定理 3.57** 若 k 是域，且 $f(x)$，$g(x)\in k[x]$，则它们的最大公因子 $d(x)$是 $f(x)$和 $g(x)$的一个线性组合．

注 根据线性组合的概念，我们现在是指 $sf+tg$，其中 $s=s(x)$，$t=t(x)$都是$k[x]$中的多项式． ◀

证明 我们可假设 f 与 g 至少有一个不为零(否则最大公因子是 0)．考虑由所有线性组合构成的集合 I：

$$I=\{s(x)f(x)+t(x)g(x):s(x),t(x)\in k[x]\}.$$

现在 f，$g\in I$(取 $s=1$，$t=0$，或 $t=1$，$s=0$)．于是，若 $N=\{n\in\mathbb{N}:n=\deg(h)$，其中 $h(x)\in I\}$，则 N 非空．由最小数原理，N 含有一个最小整数，不妨设为 n，且存在某个次数为 n 的多项式 $d(x)\in I$．若需要我们可以用 $a_n^{-1}d(x)$代替 $d(x)$，其中 a_n 是 $d(x)$的首项系数，这样我们可以假设 $d(x)$是首一的．我们断言 $d(x)$是 $f(x)$，$g(x)$的最大公因子．

由于 $d\in I$，所以 d 是 f 与 g 的一个线性组合：

$$d=sf+tg.$$

让我们通过验证 d 整除 f 和 g 来证明 d 是一个公因子．由除法算式得 $f=qd+r$，其中 $r=0$ 或 $\deg(r)<\deg(d)$．若 $r\neq0$，则

$$r=f-qd=f-q(sf+tg)=(1-qs)f-qtg\in I,$$

此与在 f 与 g 的所有线性组合中 d 的次数是最小的矛盾．因而 $r=0$，$d\mid f$．类似的讨论可证明 $d\mid g$．

最后，若 c 是 f 与 g 的一个公因子，则 c 整除 $d=sf+tg$．但是 $c\mid d$ 表明 $\deg(c)\leqslant\deg(d)$．因此 d 是 f 与 g 的最大公因子． ■ 258

→ **推论 3.58** 设 k 是域，$f(x)$，$g(x)\in k[x]$．

(i)首一公因子 $d(x)$是最大公因子当且仅当 $d(x)$能被每个公因子整除．

(ii)任何两个多项式 $f(x)$和 $g(x)$都有唯一的最大公因子．

证明 必要性已经被证明了(见定理 3.57 的证明的最后一段)：若 $d(x)$是最大公因子，则 f 和 g 的每个公因子 c 都是 $d=sf+tg$ 的因子．

反之，设 d 是 f 与 g 的一个最大公因子，设 d'是能被任意公因子 c 整除的公因子，则 $d\mid d'$．另一方面，因为 d 能被每个公因子整除(根据刚讨论过的必要性)，所以 $d'\mid d$．根据命题 3.15(因为 $k[x]$是整环)，存在单位 $u(x)\in k[x]$使得 $d'(x)=u(x)d(x)$．由习题 3.32 知 $u(x)$是一个非零常数，称之为 u．这样，$d'(x)=ud(x)$．若 d'和 d 的首项系数分别是 s'和 s，则$s'=us$．但 $d(x)$和 $d'(x)$都是首一的，于是 $u=1$，$d(x)=d'(x)$．最后的讨论也证明了最大公因子的唯一性． ■

如果我们注意一下推论 1.36 和推论 3.58，就可以在任意整环中定义最大公因子的概念.

→　**定义**　设 R 是一个整环，a，$b\in R$. 若 $a=0=b$，则定义它们的**最大公因子**为 0. 若 a，b 至少有一个非零，则定义它们的**最大公因子**为 $d\in R$，要求 d 是公因子且对每个公因子 $c\in R$ 有 $c\mid d$. a，b 的最大公因子记为(a, b).

习题 3.81 给出一个整环的例子，它含有一对没有最大公因子的元素.

刚给出的最大公因子的定义与$\mathbb{Z}$中(在第 1 章中)最大公因子的定义不完全相同，因为目前的定义不要求最大公因子是非负的. 例如，在新的定义中 4 和 6 的最大公因子是 2 和 -2. 类似地，在 $k[x]$中，新的最大公因子的定义也不同于早先给出的定义，因为目前的定义不要求最大公因子是首一的. 为了使最大公因子唯一，所以$\mathbb{Z}$中的最大公因子定义为非负的，$k[x]$中的最大公因子定义为首一的. 然而，在更一般的整环中，最大公因子是不唯一的. 若 d 和 d' 都是整环 R 中元素 a，b 的最大公因子，则存在单位 $u\in R$ 使得 $d'=ud$ (因为彼此整除). 在$\mathbb{Z}$中，最大公因子对正负号是唯一的(因为单位仅为±1)，我们选择正的最大公因子作为我们的喜爱. 在 $k[x]$中(k 是域)，两个最大公因子仅相隔一个非零常数倍(因为单位仅为非零常数)，我们选择首一多项式作为我们的喜爱. 但是，在一般的整环中，没有让人喜爱的选择，所以我们不能从最大公因子中挑出一个. 根据命题 3.41，a，b 的两个最大公因子 d 和 d'生成的主理想是相
259 同的：$(d')=(d)$. 这样，虽然 a，b 的最大公因子不唯一，但是它们决定相同的主理想.

定理 3.40 是说$\mathbb{Z}$中的每个理想都是主理想. 下面有一个类似的结论且有相同的证法.

→　**定理 3.59**　*若 k 是域，则 $k[x]$中的每个理想 I 都是主理想. 而且，若 $I\neq\{0\}$，则存在唯一的首一多项式生成 I.*

证明　若 $I=\{0\}$，则取 $d=0$. 若 I 中有非零多项式，则最小数原理允许我们选取一个次数最小的多项式 $d(x)\in I$. 若必要则用 $a^{-1}d(x)$代替 $d(x)$，其中 a 是 $d(x)$的首项系数，因此我们可以假设 $d(x)$是首一的.

我们断言 I 中每个 f 是 d 的一个倍数. 由除法算式知存在多项式 q 和 r 使得 $f=qd+r$，其中 $r=0$ 或 $\deg(r)<\deg(d)$. 根据理想定义中的(iii)，由 $d\in I$ 得 $qd\in I$，又由理想定义中的(ii)得 $r=f-qd\in I$. 若 $r\neq0$，则 r 有次数且 $\deg(r)<\deg(d)$，此与 d 在 I 中的所有多项式中次数是最小的矛盾. 因此，$r=0$，f 是 d 的倍数.

最后，$d(x)$是唯一的，若 $d'(x)$是另一个首一多项式满足$(d)=(d')$，则由命题 3.41 知 $d=d'$，因此$d(x)$是唯一的. ■

由定理 3.57 的证明可知：在 $k[x]$中，$f(x)$和 $g(x)$的最大公因子(至少有一个不是零多项式)等同于由 $f(x)$和 $g(x)$的所有线性组合构成的理想 $I=(f(x), g(x))$的首一生成元. 回忆例 3.39 中介绍的记号：若 $b_1, \cdots, b_n\in R$，则它们的所有线性组合构成的理想记为$(b_1, \cdots, b_n)$. 定理 3.57 的证明把 $k[x]$中 $f(x)$与 $g(x)$(当它们至少有一个不为零多项式时)的最大公因子与由 $f(x)$与 $g(x)$的所有线性组合构成的理想 $I=(f(x), g(x))$的首一生成元看成是相同的. 这解释了为什么用(f, g)来记最大公因子. 注意，甚至当 $f(x)$与 $g(x)$都是零多项式时，这个记号也是有意义的：最大公因子是 0，它是理想$(0, 0)=\{0\}$的生成元.

→　**定义**　交换环 R 称为**主理想整环**(简记为 PID)，若 R 是整环且它的每个理想都是主理想.

例 3.60 (i)根据定理 3.40，整数环$\mathbb{Z}$是一个主理想整环.

(ii)根据命题 3.43，每个域是主理想整环.

(iii)若 k 是一个域，则根据定理 3.59，多项式环 $k[x]$是主理想整环.

(iv)若 k 是一个域，则根据习题 3.72，形式幂级数环 $k[[x]]$是主理想整环.

(v)除$\mathbb{Z}$和 $k[x]$(k 是域)之外，还有其他的环有除法算式，高斯整数环$\mathbb{Z}[i]$就是一个例子. 这些环都称为欧几里得环，它们也是主理想整环(见命题 3.78). ◀ 260

任意交换环中的理想不一定是主理想.

例 3.61 (i)设 $R=\mathbb{Z}[x]$，即$\mathbb{Z}$上所有多项式构成的交换环. 易见常数项为偶数的多项式构成的集合 I 是$\mathbb{Z}[x]$中的理想. 我们现在证明 I 不是主理想.

假设存在 $d(x)\in\mathbb{Z}[x]$使得 $I=(d(x))$. 因为常数 $2\in I$，所以存在 $f(x)\in\mathbb{Z}[x]$使得 $2=d(x)f(x)$. 由于积的次数是因子的次数之和，所以 $0=\deg(2)=\deg(d)+\deg(f)$. 因为次数是非负的，所以 $\deg(d)=0$，即 $d(x)$是一个非零常数. 因为这里的常数都是整数，所以 $d(x)$只能为±1，±2. 因为 $d(x)\in I$，而±1不是偶数，所以 $d(x)$只能为±2. 由于 $x\in I$，所以存在 $g(x)\in\mathbb{Z}[x]$使得 $x=d(x)g(x)=\pm2g(x)$. 但右边的每个系数都是偶数，而左边 x 的系数是 1，矛盾. 因此，这样的 $d(x)$不存在，即理想 I 不是主理想.

(ii)由习题 3.75 知 $k[x, y]$不是主理想整环，其中 k 是域. 更具体地讲，可以证明理想(x, y)不是主理想. ◀

例 3.62 若 I 和 J 都是交换环 R 中的理想，我们现在证明 $I\cap J$ 也是 R 中的理想. 由于 $0\in I, 0\in J$，所以 $0\in I\cap J$. 若 $a, b\in I\cap J$，则 $a-b\in I$，$a-b\in J$，所以 $a-b\in I\cap J$. 若 $a\in I\cap J$，$r\in R$，则 $ra\in I$，$ra\in J$，因而 $ra\in I\cap J$. 因此 $I\cap J$ 是理想. 稍作改变，类似的讨论也可以证明 R 中的任一族理想(可能无限个)的交也是 R 中的理想. ◀

定义 设 $f(x)$，$g(x)\in k[x]$，其中 k 是域，则**公倍数**是指一个多项式 $m(x)\in k[x]$，可使 $f(x)\mid m(x)$和 $g(x)\mid m(x)$.

给定 $k[x]$中的非零多项式 $f(x)$，$g(x)$，定义它们的**最小公倍数**(简记为 lcm)为次数最小的那个首一公倍数. 若 $f(x)=0$ 或 $g(x)=0$，则定义它们的最小公倍数为 0. $f(x)$和 $g(x)$的最小公倍数通常记为

$$[f(x), g(x)].$$

命题 3.63 假设 k 是域，$f(x)$，$g(x)\in k[x]$不为零.

(i)$[f(x), g(x)]$是$(f(x))\cap(g(x))$的首一生成元. 261

(ii)设 $m(x)$是 $f(x)$和 $g(x)$的首一公倍数，则 $m(x)=[f(x), g(x)]$当且仅当 $m(x)$整除 $f(x)$和 $g(x)$的每个公倍数.

(iii)每对多项式 $f(x)$和 $g(x)$有唯一的最小公倍数.

证明 (i)因为 $f(x)\neq0$，$g(x)\neq0$，所以 $0\neq fg\in(f)\cap(g)$，所以$(f)\cap(g)\neq0$. 由定理 3.59，$(f)\cap(g)=(m)$，其中 m 是$(f)\cap(g)$中次数最小的首一多项式. 因 $m\in(f)$，所以存在某个 $q(x)\in k[x]$使得 $m=qf$，所以 $f\mid m$. 类似地，$g\mid m$，所以 m 是 f 和 g 的一个公倍数. 若 M 是另一个公倍数，则 $M\in(f)$，$M\in(g)$，因而 $M\in(f)\cap(g)=(m)$，所以 $m\mid M$.

因此 $\deg(m)\leqslant\deg(M)$，$m=[f,g]$.

(ii)我们刚才证明了$[f,g]$整除 f 和 g 的每个公倍数. 反之，假设 m'是能整除每个公倍数的首一公倍数. 因为$[f,g]$是一个公倍数，所以 $m'\mid[f,g]$，而由(i)知$[f,g]\mid m'$. 由命题 3.15 知存在单位 $u(x)\in k[x]$使得 $m'(x)=u(x)m(x)$. 由习题 3.32，$u(x)$是非零常数. 由于 $m(x)$和 $m'(x)$都是首一的，于是 $m(x)=m'(x)$.

(iii)若 ℓ 和 ℓ'都是 $f(x)$和 $g(x)$的最小公倍数，则由(ii)知它们彼此能够整除对方. 因为 ℓ 和 ℓ'都是首一的，根据命题 3.15 可得唯一性. ■

这里有一个素数概念的推广.

→ **定义** 交换环 R 中的元素 p 称为是**不可约的**，若 p 不是 0 也不是单位，且对 R 中的任意因子分解 $p=ab$ 要求 a 或 b 是单位.

$\mathbb{Z}$ 中的不可约元素是 $\pm p$，其中 p 是素数. 下面的命题描述了 $k[x]$中的不可约多项式，其中 k 是域.

→ **命题 3.64** 设 k 是域，则一个非常数多项式 $p(x)\in k[x]$在 $k[x]$中是不可约的当且仅当在 $k[x]$中没有如下的因子分解：$p(x)=f(x)g(x)$，其中 $\deg(f)$，$\deg(g)<\deg(p)$.

证明 若 $p(x)$是不可约的，则它一定是非常数的. 假设在 $k[x]$中 $p(x)=f(x)g(x)$，其中两个因子的次数都小于 $\deg(p)$，则 $\deg(f)$和 $\deg(g)$都不等于 0，因此两个因子都不是 $k[x]$中的单位. 这是一个矛盾.

反之，若 $p(x)$不能分解为两个更低次数的多项式的乘积，则它的因子仅形如 a 或 $ap(x)$，其中 a 是非零常数. 因为 k 是域，所以非零常数是单位，因此 $p(x)$是不可约的. ■

若 R 不是域，则不可约多项式的特性不适用于多项式环 $R[x]$. 在$\mathbb{Q}[x]$中，多项式
262 $f(x)=2x+2=2(x+1)$是不可约的，这是因为域上的线性多项式都是不可约的，这里 2 是 $\mathbb{Q}[x]$中的单位. 然而，在$\mathbb{Z}[x]$中，$f(x)$不是不可约的，这是因为 2 和 $x+1$ 都不是$\mathbb{Z}[x]$中的单位.

线性多项式 $f(x)\in k[x]$总是不可约的，其中 k 是域[若 $f=gh$，则 $1=\deg(f)=\deg(g)+\deg(h)$，因此 g 和 h 中必有一个的次数为 0 而另一个的次数为 $1=\deg(f)$]. 存在域上的多项式环，只有线性多项式是不可约多项式. 例如，由代数基本定理知$\mathbb{C}[x]$是这样的环.

像在交换环 R 中整除性的定义依赖于 R 一样，多项式 $p(x)\in k[x]$的不可约性也依赖于交换环 $k[x]$甚至依赖于域 k. 例如，$p(x)=x^2-2$ 在$\mathbb{Q}[x]$中是不可约的，但它在$\mathbb{R}[x]$中可以因子分解为$(x+\sqrt{2})(x-\sqrt{2})$.

→ **命题 3.65** 设 k 是域，$f(x)\in k[x]$是二次或三次多项式. 则 $f(x)$在 $k[x]$中是不可约的当且仅当 $f(x)$在 k 中没有根.

证明 假设 $f(x)$在 k 中有一个根 a，则由命题 3.49 知 $f(x)$有一个真正的因子分解，因此它不是不可约的，矛盾.

反之，假设 $f(x)$不是不可约的，即在 $k[x]$中存在一个因子分解 $f(x)=g(x)h(x)$满足 $\deg(g)<\deg(f)$，$\deg(h)<\deg(f)$. 根据引理 3.18 知 $\deg(f)=\deg(g)+\deg(h)$. 因为 $\deg(f)=2$ 或 3，所以 $\deg(g)$，$\deg(h)$中必有一个为 1，这样由命题 3.49 知 $f(x)$在 k 中有一个根，矛盾. ■

对次数很大的多项式来说，上述命题不成立. 例如，

$$x^4+2x^2+1=(x^2+1)^2$$

显然在$\mathbb{R}[x]$中可分解，但没有实根.

→ **命题 3.66** 设 k 是域，则每个非常数多项式 $f(x)\in k[x]$都有一个因子分解

$$f(x)=ap_1(x)\cdots p_t(x),$$

其中 a 是非零常数，$p_i(x)$是首一不可约多项式.

证明 我们对 $\deg(f)\geqslant 1$ 用第二归纳法证明该命题. 若 $\deg(f)=1$，则 $f(x)=ax+c=a(x+a^{-1}c)$. 因为每个线性多项式都是不可约的，所以 $x+a^{-1}c$ 是不可约的，因此 $f(x)$是不可约多项式的乘积. 现在假设 $\deg(f)\geqslant 1$. 若 $f(x)$是不可约的且首项系数是 a，则写 $f(x)=a(a^{-1}f(x))$，因为 $a^{-1}f(x)$是首一的，所以证毕. 若 $f(x)$不是不可约的，则 $f(x)=g(x)h(x)$，其中 $\deg(g)<\deg(f)$，$\deg(h)<\deg(f)$. 根据归纳假设，存在因子分解 $g(x)=bp_1(x)\cdots p_m(x)$和 $h(x)=cq_1(x)\cdots q_n(x)$，其中这些 p_i，q_j 是首一多项式. 于是 $f(x)=(bc)p_1(x)\cdots p_m(x)q_1(x)\cdots q_n(x)$，符合要求. ■ 263

设 k 是域，易见若 $p(x)$，$q(x)\in k[x]$都是不可约的，则 $p(x)\mid q(x)$当且仅当存在一个单位 u 使得 $q(x)=up(x)$. 另外，若 $p(x)$和 $q(x)$都是首一的，则由 $p(x)\mid q(x)$可推出 $p(x)=q(x)$. 这里有一个类似于命题 1.34 的结论.

引理 3.67 设 k 是域，$p(x)$，$f(x)\in k[x]$，令 $d(x)=(p,f)$. 若 $p(x)$是首一不可约多项式，则

$$d(x)=\begin{cases}1 & \text{当 } p(x)\nmid f(x)\\ p(x) & \text{当 } p(x)\mid f(x).\end{cases}$$

证明 $p(x)$的首一因子只有 1 和 $p(x)$. 若 $p(x)\mid f(x)$，则 $d(x)=p(x)$，因为 $p(x)$是首一的. 若 $p(x)\nmid f(x)$，则仅有的首一公因子是 1，所以 $d(x)=1$. ■

→ **定理 3.68 (欧几里得引理)** 设 k 是域，$f(x)$，$g(x)\in k[x]$. 若 $p(x)$是 $k[x]$中不可约多项式，且 $p(x)\mid f(x)g(x)$，则 $p(x)\mid f(x)$或 $p(x)\mid g(x)$. 更一般地，若 $p(x)\mid f_1(x)\cdots f_n(x)$，其中 $n\geqslant 2$，则对某个 i 有 $p(x)\mid f_i(x)$.

证明 若 $p\mid f$，则已证毕. 若 $p\nmid f$，则由引理知 $\gcd(p,f)=1$. 因此存在多项式 $s(x)$，$t(x)$使得 $1=sp+tf$，所以

$$g=spg+tfg.$$

由于 $p\mid fg$，所以 $p\mid g$. 对 $n\geqslant 2$ 用归纳法可证明第二个命题成立. ■

→ **定义** 设 k 是域，称两个多项式 $f(x)$，$g(x)\in k[x]$ **互素**，若它们的最大公因子为 1.

推论 3.69 设 k 是域，$f(x)$，$g(x)$，$h(x)\in k[x]$，并设 $h(x)$和 $f(x)$互素. 若 $h(x)\mid f(x)g(x)$，则 $h(x)\mid g(x)$.

证明 根据题设，存在某个 $q(x)\in k[x]$使得 $fg=hq$. 因为存在多项式 s，t 使得 $1=sf+th$，所以 $g=sfg+thg=shq+thg=h(sq+tg)$，这样 $h\mid g$. ■

定义 设 k 是域，有理函数 $f(x)/g(x)\in k(x)$称为**既约形式**，若 $f(x)$和 $g(x)$互素. 264

命题 3.70 设 k 是域，则每个非零的 $f(x)/g(x)\in k(x)$可以写成既约形式.

证明 若 $d=(f, g)$，则在 $k[x]$中，$f=df'$，$g=dg'$. 另外 f'和 g'互素，这是因为若 h 是 f'和 g'的非常数公因子，则 hd 会是 f 和 g 的次数比 d 更大的公因子. 现在 $f/g=df'/dg'=f'/g'$，后者是既约形式. ■

这里也出现了曾在Z中出现过的关于计算最大公因子的抱怨，但这里有相同的解决方法.

→ **定理 3.71（欧几里得算法）** *若 k 是域，$f(x)$，$g(x)\in k[x]$，则存在一个计算 $\gcd(f(x), g(x))$的算法以及求一对多项式 $s(x)$，$t(x)$使得$(f, g)=sf+tg$ 的算法.*

证明 只要重复Z中欧几里得算法的证明即可：反复应用除法算式.

$$\begin{aligned} g &= q_0 f + r_1 & \deg(r_1) &< \deg(f) \\ f &= q_1 r_1 + r_2 & \deg(r_2) &< \deg(r_1) \\ r_1 &= q_2 r_2 + r_3 & \deg(r_3) &< \deg(r_2) \\ r_2 &= q_3 r_3 + r_4 & \deg(r_4) &< \deg(r_3) \\ &\vdots & &\vdots \end{aligned}$$

像定理 1.44 的证明一样，最后一个非零余式是公因子且能被每个公因子整除. 因为余式可能不首一（即使 f 和 g 都首一，余式 $r=g-qf$ 也可能不首一），所以我们必须通过用它的首项系数的逆元乘以它来使得它是首一的. ■

例 3.72 在$\mathbb{Q}[x]$中用欧几里得算法求 $\gcd(x^5+1, x^3+1)$.

$$\begin{aligned} x^5+1 &= x^2(x^3+1)+(-x^2+1) \\ x^3+1 &= (-x)(-x^2+1)+(x+1) \\ -x^2+1 &= (-x+1)(x+1). \end{aligned}$$

这样 $x+1$ 是 gcd. ◀

例 3.73 在$\mathbb{Q}[x]$中求

265 $$f(x)=x^3-x^2-x+1 \quad \text{和} \quad g(x)=x^3+4x^2+x-6.$$

的 gcd. 注意 $f(x)$，$g(x)\in \mathbb{Z}[x]$，且Z 不是域. 在求解的过程中，有理数可能加入，因为Q是包含Z 的最小域. 看以下等式：

$$\begin{aligned} g &= 1\cdot f+(5x^2+2x-7) \\ f &= \left(\frac{1}{5}x-\frac{7}{25}\right)(5x^2+2x-7)+\left(\frac{24}{25}x-\frac{24}{25}\right) \\ 5x^2+2x-7 &= \left(\frac{25}{24}5x+\frac{175}{24}\right)\left(\frac{24}{25}x-\frac{24}{25}\right). \end{aligned}$$

由此得到最大公因子是 $x-1$ $\left[\text{是将}\frac{24}{25}x-\frac{24}{25}\text{化为首一的}\right]$. 读者应该可以求出 $s(x)$，$t(x)$使得 $x-1$表示为一个线性组合（和在算术中一样，从底行开始算起）.

作为一个计算工具，我们可以在任何一步把分母清除. 例如，我们可以把上述第二个方程替换为

$$(5x-7)(5x^2+2x-7)+(24x-24);$$

毕竟，我们最终要用一个单位相乘来得到首一的最大公因子. ◀

例 3.74　在$\mathbb{F}_5[x]$中求

$$f(x) = x^3 - x^2 - x + 1 \quad 和 \quad g(x) = x^3 + 4x^2 + x - 6$$

的 gcd. 欧几里得算法可以适当地简化.

$$g = 1 \cdot f + (2x + 3)$$
$$f = (3x^2 + 2)(2x + 3).$$

最大公因子是 $x-1$（是将 $2x+3$ 化为首一的）. ◀

以下是例 3.73 中多项式 $f(x)$和 $g(x)$的因子分解：

$$f(x) = x^3 - x^2 - x + 1 = (x-1)^2(x+1)$$

和

$$g(x) = x^3 + 4x^2 + x - 6 = (x-1)(x+2)(x+3).$$

如果一开始我们就知道了这些因子分解，那么就可以看到 $x-1$ 是最大公因子. 这说明了算术基本定理的一个类似结论提供了另一种计算最大公因子的方法. 这样一个类似结论确实存在（见命题 3.86）. 但是，在可操作性上，分解多项式是一项很复杂的工作，且欧几里得算法是计算最大公因子的最好方法.

以下是从欧几里得算法中得到的一个出人意料的结果. 266

→ **推论 3.75**　设 k 是域 K 的一个子域，则 $k[x]$是 $K[x]$的一个子环. 若 $f(x)$，$g(x) \in k[x]$，则它们在 $k[x]$中的最大公因子与它们在 $K[x]$中的最大公因子相等.

证明　由 $K[x]$中的除法算式得

$$g(x) = Q(x)f(x) + R(x),$$

其中 $Q(x)$，$R(x) \in K[x]$，并且 $R(x)=0$ 或 $\deg(R)<\deg(f)$. 由于 $f(x)$，$g(x)\in k[x]$，所以由 $k[x]$中的除法算式得

$$g(x) = q(x)f(x) + r(x),$$

其中 $q(x)$，$r(x)\in k[x]$，并且 $r(x)=0$ 或 $\deg(r)<\deg(f)$. 因为 $k[x]\subseteq K[x]$，所以等式 $g(x)=q(x)f(x)+r(x)$在 $K[x]$中也成立，由 $K[x]$中除法算式的商式和余式的唯一性知 $Q(x)=q(x)\in k[x]$和 $R(x)=r(x)\in k[x]$. 因此，$K[x]$中欧几里得算法中的等式与小环 $k[x]$中欧几里得算法中的等式是相同的. 所以在两个多项式环中获得相同的最大公因子. ■

尽管在$\mathbb{C}[x]$中因子更多，但无论是在$\mathbb{R}[x]$中还是在$\mathbb{C}[x]$中，x^3-x^2+x-1 和 x^4-1 的最大公因子都是 x^2+1.

当 k 是域时，我们已经看到，对$\mathbb{Z}$ 证明的定理，对 $k[x]$也有许多类似的结论. 根本的原因是两个环都是 PID.

欧几里得环

除$\mathbb{Z}$ 和 $k[x]$（k 是域）外，还有其他的环有除法算式. 特别地，我们给出这样的一个环的例子，它的除法算式中的商式和余式是不唯一的. 我们首先推广$\mathbb{Z}$ 和 $k[x]$共有的一个性质.

定义　交换环 R 称为**欧几里得环**，若 R 是整环，且存在一个函数

$$\partial : R^\times \to \mathbb{N}$$

（其中 $R^\times$ 表示 R 的所有非零元素构成的集合），称为**次数函数**，满足

(i)对所有 f, $g\in R^\times$, 有 $\partial(f)\leqslant\partial(fg)$;

(ii)对所有 f, $g\in R$ 且 $f\in R^\times$, 存在 q, $r\in R$ 使得

$$g = qf + r,$$

267 其中 $r=0$ 或 $\partial(r)<\partial(f)$.

例 3.76 (i)任意域 R 都是欧几里得环且次数函数 ∂ 等于 0: 若 $g\in R$, $f\in R^\times$, 则令 $q=f^{-1}$, $r=0$. 反之, 若 R 是整环且零函数 $\partial: R^\times\to\mathbb{N}$ 是一个次数函数, 则 R 是域. 若 $f\in R^\times$, 则存在 q, $r\in R$ 使得 $1=qf+r$. 假设 $r\neq 0$, 则 $\partial(r)<\partial(f)=0$, 矛盾. 因此 $r=0$ 且 $1=qf$, 这样 f 是一个单位. 因此 R 是域.

(ii)整环 $\mathbb{Z}$ 是欧几里得环且次数函数是 $\partial(m)=|m|$. 在 $\mathbb{Z}$ 中, 我们有

$$\partial(mn) = |mn| = |m||n| = \partial(m)\partial(n).$$

(iii)当 k 是域时, 整环 $k[x]$ 是欧几里得环且次数函数是非零多项式通常的次数. 在 $k[x]$ 中, 我们有

$$\begin{aligned}\partial(fg) &= \deg(fg)\\ &= \deg(f)+\deg(g)\\ &= \partial(f)+\partial(g)\\ &\geqslant \partial(f).\end{aligned}$$

一个特殊的次数函数的某些性质不一定对所有次数函数都成立. 例如, 在(ii)中, $\mathbb{Z}$ 中的次数函数是乘法的: $\partial(mn)=\partial(m)\partial(n)$, 而 $k[x]$ 中的次数函数不是乘法的. 若次数函数 ∂ 是乘法的, 即, 若

$$\partial(fg) = \partial(f)\partial(g),$$

则 ∂ 称为**欧几里得范数**. ◀

例 3.77 高斯[⊖]整数环 $\mathbb{Z}[i]$ 构成一个欧几里得环, 它的次数函数

$$\partial(a+bi) = a^2+b^2$$

是一个欧几里得范数.

为证明次数函数 ∂ 是乘法的, 我们首先应该注意: 若 $\alpha=a+bi$, 则

$$\partial(\alpha) = \alpha\bar{\alpha},$$

其中 $\bar{\alpha}=a-bi$ 是 α 的复共轭. 于是对所有 α, $\beta\in\mathbb{Z}[i]$ 有 $\partial(\alpha\beta)=\partial(\alpha)\partial(\beta)$, 这是因为

$$\partial(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \partial(\alpha)\partial(\beta).$$

268 事实上, 根据推论 1.23, 它甚至对所有 α, $\beta\in\mathbb{Q}[i]=\{x+yi: x, y\in\mathbb{Q}\}$ 都成立.

我们现在证明 ∂ 满足次数函数的第一条性质. 若 $\beta=c+di\in\mathbb{Z}[i]$ 且 $\beta\neq 0$, 则

$$1\leqslant\partial(\beta),$$

这是因为 $\partial(\beta)=c^2+d^2$ 是正整数. 于是, 若 α, $\beta\in\mathbb{Z}[i]$ 且 $\beta\neq 0$, 则

$$\partial(\alpha)\leqslant\partial(\alpha)\partial(\beta) = \partial(\alpha\beta).$$

下面证明 ∂ 也满足第二条性质. 给定 α, $\beta\in\mathbb{Z}[i]$ 且 $\beta\neq 0$, 把 α/β 看作是 $\mathbb{C}$ 的一个元素. 有理化分母, 得 $\alpha/\beta=\alpha\bar{\beta}/\beta\bar{\beta}=\alpha\bar{\beta}/\partial(\beta)$, 所以

⊖ 之所以叫做高斯整数是因为高斯一直利用 $\mathbb{Z}[i]$ 和它的欧几里得范数 ∂ 去研究四次剩余.

$$\alpha/\beta = x + yi,$$

其中 x，$y \in \mathbb{Q}$．记 $x=m+u$，$y=n+v$，其中 m，$n \in \mathbb{Z}$ 分别是最接近 x 和 y 的整数．这样 $|u|$，$|v| \leqslant \frac{1}{2}$．$\left[\text{若 } x \text{ 或 } y \text{ 形如 } m+\frac{1}{2}\right.$，其中 m 为整数，则有一个最接近于整数的选取：$x=m+\frac{1}{2}$ 或 $x=(m+1)-\frac{1}{2}$；若 x 或 y 形如 $m-\frac{1}{2}$，则选取类似．$\left.\right]$于是

$$\alpha = \beta(m + ni) + \beta(u + vi).$$

注意 $\beta(u+vi) \in \mathbb{Z}[i]$，这是因为它等于 $\alpha - \beta(m+ni)$．最后，我们有 $\partial(\beta(u+vi)) = \partial(\beta)\partial(u+vi)$，所以若 $\partial(u+vi)<1$，则 ∂ 是一个次数函数．它确实是，因为由不等式 $|u| \leqslant \frac{1}{2}$ 和 $|v| \leqslant \frac{1}{2}$ 得 $u^2 \leqslant \frac{1}{4}$ 和 $v^2 \leqslant \frac{1}{4}$，因而 $\partial(u+vi) = u^2+v^2 \leqslant \frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1$．因此 $\partial(\beta(u+vi)) < \partial(\beta)$，所以 $\mathbb{Z}[i]$ 是一个欧几里得环，其次数函数是欧几里得范数．

高斯整数环 $\mathbb{Z}[i]$ 是欧几里得环，但在 $\mathbb{Z}[i]$ 中商式和余式可能不唯一[⊖]．例如，设 $\alpha=3+5i$，$\beta=2$，则 $\alpha/\beta=\frac{3}{2}+\frac{5}{2}i$．选取是：

$$m = 1 \text{ 和 } u = \frac{1}{2} \quad \text{或} \quad m = 2 \text{ 和 } u = -\frac{1}{2};$$

$$n = 2 \text{ 和 } v = \frac{1}{2} \quad \text{或} \quad n = 3 \text{ 和 } v = -\frac{1}{2}.$$

这样，$\mathbb{Z}[i]$ 中用 2 除 $3+5i$ 后得到 4 个商式，并且每个余式(例如 $1+i$)的次数为 $2<4=\partial(2)$：

$$\begin{aligned} 3 + 5i &= 2(1 + 2i) + (1 + i) \\ &= 2(1 + 3i) + (1 - i) \\ &= 2(2 + 2i) + (-1 + i) \\ &= 2(2 + 3i) + (-1 - i). \end{aligned}$$ 269

◀

命题 3.78 *每个欧几里得环 R 都是一个 PID．特别地，高斯整数环 $\mathbb{Z}[i]$ 是一个 PID．*

证明 改写命题 3.59 的证明即可：若 I 是 R 中的非零理想，则 $I=(d)$，其中 d 是 I 中次数最小的那个元素． ■

命题 3.78 的逆命题不成立：有一些 PID 不是欧几里得环，请看下面一个例子．

例 3.79 在代数数理论中，我们证明了环

$$\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$$

是一个 PID，其中 $\alpha=\frac{1}{2}(1+\sqrt{-19})$[$\alpha$ 是 x^2-x+5 的根，$\mathbb{Z}[\alpha]$ 是二次数域 $\mathbb{Q}(\alpha)$ 中的代数整数环]．1949 年，默慈金(T. S. Motzkin)证明了 $\mathbb{Z}[\alpha]$ 不是欧几里得环．为了证明这个，他找到了欧几里得环的下述性质，但没有提到它的次数函数． ◀

⊖ 注意 $\mathbb{Z}$ 中的下列等式：

$$3=1\cdot 2+1,$$
$$3=2\cdot 2-1.$$

现在 $|-1|=|1|<|2|$，所以在 $\mathbb{Z}$ 中商式和余式是不唯一的！在定理 1.32 中，我们要求余数是非负的从而保证唯一性成立．

定义 整环 R 中的元素 u 称为**通用侧因子**，若 u 不是单位，且对每个 $x\in R$ 来说，要么 $u\mid x$ 要么存在一个单位 $z\in R$ 使得 $u\mid(x+z)$.

命题 3.80 若 R 是欧几里得环但不是域，则 R 有一个通用侧因子.

证明 定义

$$S=\{\partial(v): v\neq 0 \text{ 且 } v \text{ 不是单位}\},$$

其中 ∂ 是 R 上的次数函数. 因为 R 不是域，所以存在某个 $v\in R^{\times}$ 不是单位，所以 S 是自然数集的一个非空子集. 根据最小数原理，存在一个非单位元素 $u\in R^{\times}$ 使得 $\partial(u)$ 是 S 的最小元. 我们断言 u 就是通用侧因子. 若 $x\in R$，则存在元素 q 和 r 使得 $x=qu+r$，其中 $r=0$ 或 $\partial(r)<\partial(u)$. 若 $r=0$，则 $u\mid x$；若 $r\neq 0$，则 r 一定是单位，否则它的存在与 $\partial(u)$ 是 S 中的最小数矛盾. 所以证明了 u 是通用侧因子. ■

默慈金随后证明了环 $\mathbb{Z}[\alpha]=\{a+b\alpha: a, b\in\mathbb{Z}\}$ 没有通用侧因子，其中 $\alpha=\frac{1}{2}(1+\sqrt{-19})$，

270 并由此得出这个主理想整环 $\mathbb{Z}[\alpha]$ 不是欧几里得环(见习题 3.70).

下面的结论对任意 PID 都成立，我们将把该结论运用于 $\mathbb{Z}[i]$ 上.

命题 3.81 设 R 是一个 PID.

(i) 每对 $\alpha, \beta\in R$ 都有最大公因子 δ，并且 δ 是 α 和 β 的一个线性组合：存在 $\sigma, \tau\in R$ 满足

$$\delta=\sigma\alpha+\tau\beta.$$

(ii) 若不可约元素 $\pi\in R$ 整除 $\alpha\beta$，则 $\pi\mid\alpha$ 或 $\pi\mid\beta$.

证明 (i) 我们可假设 α 和 β 至少有一个不为零(否则，最大公因子是 0，结论显然是成立的). 考虑所有线性组合构成的集合 I：

$$I=\{\sigma\alpha+\tau\beta: \sigma,\tau\in R\}.$$

现在 $\alpha, \beta\in I$(取 $\sigma=1, \tau=0$ 或 $\sigma=0, \tau=1$). 易检验 I 是 R 中的一个理想，因为 R 是一个 PID，所以存在 $\delta\in I$ 使得 $I=(\delta)$. 我们断言 δ 是 α 和 β 的最大公因子.

由于 $\alpha\in I=(\delta)$，所以存在某个 $\rho\in R$ 使得 $\alpha=\rho\delta$，即 δ 是 α 的一个因子. 类似地，δ 是 β 的一个因子. 所以 δ 是 α 和 β 的一个公因子.

由于 $\delta\in I$，所以它是 α 和 β 的线性组合：存在 $\sigma, \tau\in R$ 使得

$$\delta=\sigma\alpha+\tau\beta.$$

最后，若 γ 是 α 和 β 的任一公因子，则 $\alpha=\gamma\alpha'$，$\beta=\gamma\beta'$，因为 $\delta=\sigma\alpha+\tau\beta=\gamma(\sigma\alpha'+\tau\beta')$，所以 γ 整除 δ. 由此得 δ 是最大公因子.

(ii) 若 $\pi\mid\alpha$，则证毕. 若 $\pi\nmid\alpha$，则由习题 3.77 知 1 是 π 和 α 的最大公因子. 因此存在 $\sigma, \tau\in R$ 使得 $1=\sigma\pi+\tau\alpha$，所以

$$\beta=\sigma\pi\beta+\tau\alpha\beta.$$

由于 $\pi\mid\alpha\beta$，所以 $\pi\mid\beta$，证毕. ■

若 n 是奇数，则 $n\equiv 1 \bmod 4$ 或 $n\equiv 3 \bmod 4$. 特别地，奇素数可以分为两类. 例如，5，13，17 同余于 1 mod 4，而 3，7，11 同余于 3 mod 4.

我们可以用数论的方法证明下面的引理，但我们将用学过的代数知识来证明它.

引理 3.82 若 p 是素数且 $p\equiv 1 \bmod 4$，则存在整数 m 满足

$$m^2 \equiv -1 \bmod p.$$

证明 根据定理 3.55，乘法群 $\mathbb{F}_p^\times$ 是一个循环群. 又根据命题 2.75，对 $|\mathbb{F}_p^\times| = p-1$ 的每个因子 d 来说，$\mathbb{F}_p^\times$ 都有唯一一个阶为 d 的子群. 因为 $p-1 \equiv 0 \bmod 4$，所以 $\mathbb{F}_p^\times$ 含有一个阶为 4 的子群 S. 由命题 2.73 知循环群的子群还是循环群，所以存在整数 m 满足 $S=\langle[m]\rangle$. 由于 $[m]$ 的阶为 4，所以 $[m^2]$ 的阶为 2，即 $[m^2]=[-1]$（因为 $[-1]$ 是 $\mathbb{F}_p^\times$ 中 阶为 2 的唯一元素）. 因此，$m^2 \equiv -1 \bmod p$. ■ [271]

定理 3.83（费马二平方定理）[⊖] 一个奇素数 p 是两个平方数的和，

$$p = a^2 + b^2,$$

其中 a，b 为整数，当且仅当 $p \equiv 1 \bmod 4$.

证明 对任意整数 a 有 $a \equiv r \bmod 4$，其中 $r=0, 1, 2, 3$，所以 $a^2 \equiv r^2 \bmod 4$. 但是，mod 4 时，

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 = 4 \equiv 0, 3^2 = 9 \equiv 1,$$

所以 $a^2 \equiv 0$ 或 $1 \bmod 4$. 于是，对任意整数 a，b 有 $a^2+b^2 \not\equiv 3 \bmod 4$. 因此，若 $p=a^2+b^2$，其中 a，b 为整数，则 $p \not\equiv 3 \bmod 4$. 由于 p 是奇数，所以 $p \equiv 1 \bmod 4$ 或 $p \equiv 3 \bmod 4$. 我们刚才排除了最后一种可能性，所以 $p \equiv 1 \bmod 4$.

反之，假设 $p \equiv 1 \bmod 4$. 由引理可知，存在整数 m 使得

$$p \mid (m^2+1).$$

在 $\mathbb{Z}[i]$ 中，存在一个因子分解 $m^2+1=(m+\mathrm{i})(m-\mathrm{i})$，所以在 $\mathbb{Z}[i]$ 中

$$p \mid (m+\mathrm{i})(m-\mathrm{i}).$$

若 $\mathbb{Z}[i]$ 中 $p \mid m+\mathrm{i}$，则存在整数 u，v 使得 $m+\mathrm{i}=p(u+\mathrm{i}v)$. 取复共轭，我们有 $m-\mathrm{i}=p(u-\mathrm{i}v)$，所以 $p \mid m-\mathrm{i}$. 因此，$p \mid (m+\mathrm{i})-(m-\mathrm{i})=2\mathrm{i}$，这与 $\partial(p)=p^2>\partial(2\mathrm{i})=4$ 矛盾. 由此我们断言 p 不是不可约元素，这是因为它不满足命题 3.81. 因为 $\mathbb{Z}[i]$ 是一个 PID，所以存在一个因子分解

$$p = \alpha\beta,$$

其中 $\alpha=a+\mathrm{i}b$，$\beta=c+\mathrm{i}d$ 都不是单位. 这样 $\partial(\alpha)=a^2+b^2 \neq 1$，$\partial(\beta)=c^2+d^2 \neq 1$. 因此，取范数得 $\mathbb{Z}$ 中的一个等式：

$$\begin{aligned} p^2 &= \partial(p) \\ &= \partial(\alpha\beta) \\ &= \partial(\alpha)\partial(\beta) \\ &= (a^2+b^2)(c^2+d^2). \end{aligned}$$ [272]

由于 $a^2+b^2 \neq 1$，$c^2+d^2 \neq 1$，所以由算术基本定理得 $p=a^2+b^2$（且 $p=c^2+d^2$）. ■

习题

H 3.56 判断对错并说出理由.

(i) 若 $a(x)$，$b(x) \in \mathbb{F}_5[x]$ 且 $b(x) \neq 0$，则存在 $c(x)$，$d(x) \in \mathbb{F}_5[x]$ 满足 $a(x)=b(x)c(x)+d(x)$，其中 $d(x)=0$ 或 $\deg(d)<\deg(b)$.

⊖ 费马第一个陈述了该定理，但是欧拉第一个发表了此定理的证明. 高斯证明了仅存在一对 a，b 满足 $p=a^2+b^2$.

(ii)若 $g(x)$，$f(x)\in\mathbb{Z}[x]$且 $f(x)\neq 0$，则存在 $q(x)$，$r(x)\in\mathbb{Z}[x]$满足 $g(x)=f(x)q(x)+r(x)$，其中 $r(x)=0$ 或 $\deg(r)<\deg(f)$.

(iii)$2x^2+4x+2$ 和 $4x^2+12x+8$ 在$\mathbb{Q}[x]$中的最大公因子是 $2x+2$.

(iv)若 R 是一个整环，则 $R[x]$中每个单位的次数是 0.

(v)若 k 是一个域，$p(x)\in k[x]$是一个非常数多项式且在 k 中没有根，则 $p(x)$在 $k[x]$中不可约.

(vi)对每个二次多项式 $s(x)\in\mathbb{C}[x]$，存在 a，$b\in\mathbb{C}$ 和 $q(x)\in\mathbb{C}[x]$，满足 $(x+1)^{1000}=s(x)q(x)+ax+b$.

(vii)若 $k=\mathbb{F}_p(x)$，其中 p 是一个素数，且 $f(x)$，$g(x)\in k[x]$满足对所有 $a\in k$ 有 $f(a)=g(a)$，则 $f(x)=g(x)$.

(viii)若 k 是一个域，则 $k[x]$是一个 PID.

(ix)$\mathbb{Z}$ 是一个欧几里得环.

(x)存在整数 m 满足 $m^2\equiv -1 \bmod 89$.

*3.57 在习题 3.10 中我们看到，给定一个交换环 R，则 $F(R)=\{$所有函数 $R\to R\}$在点态运算下作成一个交换环.

(i)若 R 是一个交换环，证明 $\varphi: R[x]\to\mathcal{F}(R)$，$f(x)\mapsto f^\flat$，是一个同态.

H (ii)若 k 是一个有限域，证明 φ 是一个单射.

H 3.58 求 x^2-x-2 和 x^3-7x+6 在$\mathbb{F}_5[x]$中的最大公因子，并将它表示成它们的线性组合.

*3.59 设 k 是一个域，$f(x)\in k[x]$不为零，a_1，a_2，…，a_t 是 $f(x)$在 k 中的一些不相同的根. 证明，存在 $g(x)\in k[x]$使得 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_t)g(x)$.

H 3.60 若 R 是一个整环，$f(x)\in R[x]$的次数是 n，证明 $f(x)$在 R 中至多有 n 个根.

3.61 设 R 是任意交换环. 若 $f(x)\in R[x]$且 $a\in R$ 是 $f(x)$的一个根，即 $f(a)=0$，证明 $R[x]$中存在分解式 $f(x)=(x-a)g(x)$.

3.62 证明欧几里得引理的逆命题. 设 k 是一个域，且 $f(x)\in k[x]$是次数$\geqslant 1$ 的多项式. 若只要 $f(x)$整除两个多项式的积就一定整除其中一个因子，则 $f(x)$是不可约的.

H 3.63 设 $f(x)$，$g(x)\in R[x]$，其中 R 是一个整环. 若 $f(x)$的首项系数是 R 中的一个单位，则除法算式给出 $f(x)$除 $g(x)$后的商式 $q(x)$和余式 $r(x)$. 证明 $q(x)$和 $r(x)$由 $g(x)$和 $f(x)$唯一确定.

*H 3.64 设 k 是一个域，$f(x)$，$g(x)\in k[x]$互素. 若 $h(x)\in k[x]$，证明由 $f(x)\mid h(x)$和 $g(x)\mid h(x)$可推出
273 $f(x)g(x)\mid h(x)$.

3.65 (i)证明下述伪码补充了求 $k[x]$中 $f(x)$和 $g(x)$的最大公因子的欧几里得算法，其中 k 是一个域.

```
Input: g, f
Output: d
d := g; s := f
WHILE s≠0 DO
   rem := remainder (d, s)
   d := s
s := rem
END WHILE
a := leading coefficient of d
d := a^{-1} d
```

(ii)求(f, g)，其中$f(x)=x^2+1$，$g(x)=x^3+x+1\in \mathbb{I}_3[x]$.

*H 3.66　若k是一个域且$1+1\neq 0$，证明$\sqrt{1-x^2}\notin k(x)$，其中$k(x)$是有理函数构成的域.

*H 3.67　设$f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)\in R[x]$，其中$R$是一个交换环. 证明$f(x)$没有重根(即所有$a_i$不相同)当且仅当$\gcd(f, f')=1$，其中$f'$是$f$的导数.

3.68　设∂是欧几里得环R的次数函数. 若m，$n\in \mathbb{N}$且$m\geqslant 1$，证明∂'也是R的次数函数，其中$\partial'(x)=m\partial(x)+n$对所有$x\in R$成立. 由此知欧几里得环可能没有次数为0或1的元素.

3.69　设R是欧几里得环，其次数函数是∂.

(i)证明$\partial(1)\leqslant\partial(a)$对所有非零的$a\in R$成立.

H (ii)证明非零$u\in R$是单位当且仅当$\partial(u)=\partial(1)$.

*3.70　设$\alpha=\frac{1}{2}(1+\sqrt{-19})$，$R=\mathbb{Z}[\alpha]$.

(i)证明$N: R^\times\to\mathbb{N}$，$N(m+n\alpha)=m^2-mn+5n^2$是乘法的：$N(uv)=N(u)N(v)$.

(ii)证明R中的单位只有± 1.

(iii)证明不存在满同态$R\to\mathbb{I}_2$或$R\to\mathbb{I}_3$.

(iv)假设R有次数函数$\partial: R^\times\to\mathbb{N}$. 选取$u\in R-\{0, 1, -1\}$使得$\partial(u)$是最小的. 证明，对所有$r\in R$，存在$d\in\{0, 1, -1\}$使得$r-d\in(u)$.

(v)利用环$R/(u)$去证明R不是欧几里得环.

*H 3.71　设R是一个欧几里得环，其次数函数是∂，并假设$b\in R$既不是零元也不是单位. 证明对每个$i\geqslant 0$有$\partial(b^i)<\partial(b^{i+1})$.

H 3.72　若k是一个域，证明形式幂级数环$k[[x]]$是PID.

3.73　设k是一个域，并设$k[x]$中的多项式$a_1(x)$，$a_2(x)$，…，$a_n(x)$被给定.

H (i)证明这些多项式的最大公因子$d(x)$有形式$\sum t_i(x)a_i(x)$，其中$t_i(x)\in k[x]$，$1\leqslant i\leqslant n$.

(ii)证明，若$c(x)$是这些多项式的首一公因子，则$c(x)$是$d(x)$的因子.

H 3.74　用$[f(x), g(x)]$表示$f(x)$，$g(x)\in k[x]$的最小公倍数，其中k是一个域. 证明，若$f(x)g(x)$是首一的，则

$$[f,g](f,g)=fg.$$ 274

*3.75　若k是一个域，证明$k[x, y]$中的理想(x, y)不是一个主理想.

3.76　对每个$m\geqslant 1$，证明$\mathbb{I}_m$中的每个理想都是一个主理想.(若m是合数，则$\mathbb{I}_m$不是PID，因为它不是整环.)

*H 3.77　设R是PID且$\pi\in R$是不可约元素. 若$\beta\in R$且$\pi\nmid\beta$，证明π和β互素.

3.78　H (i)证明，x，$y\in k[x, y]$互素，但1不是它们的线性组合，即不存在$s(x, y)$，$t(x, y)\in k[x, y]$使得$1=xs(x, y)+yt(x, y)$.

(ii)证明$\mathbb{Z}[x]$中2和x互素，但1不是它们的线性组合，即不存在$s(x)$，$t(x)\in\mathbb{Z}[x]$使得$1=2s(x)+xt(x)$.

H 3.79　因为$x-1=(\sqrt{x}+1)(\sqrt{x}-1)$，所以一个学生断言$x-1$不是不可约的，请说明他的错误.

3.80　(i)把5和13都分解成$\mathbb{Z}[i]$中两个非单位元素的积，并把65分解成$\mathbb{Z}[i]$中四个非单位元素的积.

(ii)用两种不同方法把65分解成两个共轭因子的积$\alpha\bar{\alpha}$. 利用这些，用两种不同的表达式把65表示成$\mathbb{Z}$中两个平方数的和.

*H 3.81　证明存在整环R，它有一对元素没有最大公因子(参看一般整环中最大公因子的定义).

→3.6 唯一分解

以下是一个类似于算术基本定理的多项式定理. 该定理表明不可约多项式是任意多项式的"建筑块", 就像素数是任意整数的建筑块一样. 为了表述简便, 让我们约定"积"可以只有一个因子. 因此, 当我们说多项式 $f(x)$是不可约多项式的积时, 我们允许积只有一个因子的可能, 即 $f(x)$本身是不可约的.

→ **定理 3.84 (唯一分解)** 若 k 是域, 则每个次数$\geqslant 1$ 的多项式 $f(x) \in k[x]$都是一个非零常数和一些首一不可约多项式的乘积. 而且, 若

$$f(x) = ap_1(x) \cdots p_m(x) \quad 和 \quad f(x) = bq_1(x) \cdots q_n(x),$$

其中 a, b 是非零常数, 所有 p_i 和 q_j 都是首一不可约多项式, 则 $a=b$, $m=n$, 且这些 q 可以重给下标使得对所有 i 有 $q_i = p_i$.

证明 在命题 3.66 中我们已经证明了多项式 $f(x) \in k[x]$可以分解为不可约多项式的乘积, 因此我们现在只需证明唯一性.

因为首一多项式的乘积是首一的, 所以等式 $f(x)=ap_1(x)\cdots p_m(x)$给出了 $f(x)$的首项系数 a. 这样, $f(x)$的两个因子分解就给出了 $a=b$, 这是因为它们都等于 $f(x)$的首项系数. 现在证明唯一性只需证明
275

$$p_1(x) \cdots p_m(x) = q_1(x) \cdots q_n(x).$$

对 $\max\{m, n\} \geqslant 1$ 用归纳法证明. 显然基础步骤是成立的, 这是因为现在给定的等式是 $p_1(x)=q_1(x)$. 对于归纳步, 给定的等式表明 $p_m(x) \mid q_1(x)\cdots q_n(x)$. 根据定理 3.68(关于多项式的欧几里得引理), 存在某个 i 使得 $p_m(x) \mid q_i(x)$. 但是 $q_i(x)$是首一不可约多项式, 除 1 和自身外没有其他的首一因子, 所以 $q_i(x)=p_m(x)$. 重新给出下标, 我们可以假设 $q_n(x)=p_m(x)$. 消去这个因子, 我们有 $p_1(x)\cdots p_{m-1}(x)=q_1(x)\cdots q_{n-1}(x)$. 根据归纳假设, $m-1=n-1$(因而$m=n$), 在重给下标后, 对所有 i 有 $q_i=p_i$. ■

例 3.85 在$\mathbb{I}_8[x]$中, 读者可以验证

$$x^2 - 1 = (x-1)(x+1) = (x-3)(x+3).$$

每个线性因子都是不可约的(当然, $\mathbb{I}_8$ 不是域). 因此, 唯一因子分解定理在$\mathbb{I}_8[x]$中不成立. ◀

注 整环 R 称为唯一因子分解整环(简记为 UFD), 若每个非零非单位元素 $r \in R$ 是一些不可约元素的乘积, 且这样的因子分解在本质上是唯一的. 例 3.10 中的整环 $\mathbb{Z}[\zeta_p]$在这一点上是非常有趣的, 其中 $\zeta=e^{2\pi i/p}$且 p 是奇素数. 满足

$$a^2 + b^2 = c^2$$

的正整数 a, b, c 称为毕达哥拉斯三元数组, 例如 3, 4, 5 和 5, 12, 13, 它们已被认识了至少四千年了, 并且在大约两千年前丢番图(Diophantus)把它们分了类(见习题 1.67). 大约在 1637 年, 费马在丢番图著的一本书的抄写本的页边空白处记下了如今称为费马大定理的结论: 对所有整数 $n \geqslant 3$, 不存在正整数 a, b, c 使得

$$a^n + b^n = c^n.$$

费马声称：他对这个结论有一个非常精彩的证明，但因空白太少而不能把它记录下来．他确实在其他地方证明了 $n=4$ 时结论成立，后来其他人证明了 n 取一些较小数时结论也成立．然而这个一般结论挑战了数学家们几百年．

称正整数 $n\geq 2$ 为费马整数，若不存在正整数 a，b，c 使得 $a^n+b^n=c^n$．若 n 是一个费马整数，则它的倍数 nk 也是费马整数．否则，存在正整数 r，s，t 使 $r^{nk}+s^{nk}=t^{nk}$，这就得到矛盾 $a^n+b^n=c^n$，其中 $a=r^k$，$b=s^k$，$c=t^k$．例如，形如 $4k$ 的任意整数都是费马整数．因为每个正整数都是素数的乘积，所以若每个奇素数是费马整数，则费马大定理成立． 276

像在习题 3.85 中一样，对某个奇素数 p，一个解 $a^p+b^p=c^p$ 给出了一个因子分解

$$c^p=(a+b)(a+\zeta b)(a+\zeta^2 b)\cdots(a+\zeta^{p-1}b),$$

其中 $\zeta=\zeta_p=e^{2\pi i/p}$．19 世纪 40 年代，库默尔(E. Kummer)在整环 $\mathbb{Z}[\zeta_p]$ 中考虑了这个因子分解(见例 3.10 中的描述)．他证明了，若唯一因子分解在 $\mathbb{Z}[\zeta_p]$ 中成立，则不存在正整数 a，b，c(任何一个都不能被 p 整除)使得 $a^p+b^p=c^p$．但是，库默尔认识到，即使唯一因子分解对某个素数 p 在 $\mathbb{Z}[\zeta_p]$ 中确实成立，它也不能在所有 $\mathbb{Z}[\zeta_p]$ 中都成立．为推广他的证明，他发明了称之为"理想数"的东西，并证明了理想数可唯一因子分解为"素理想数"的乘积．这些理想数激发了戴德金(R. Dedekind)去定义任意交换环中的理想(我们关于理想的定义就是戴德金给出的)，他还证明了特殊环 $\mathbb{Z}[\zeta_p]$ 中的理想与库默尔的理想数相对应．这些年来这些研究已经有了巨大的发展．1995 年，威尔斯(A. Wiles)证明了费马大定理．

设 k 是一个域，$f(x)\in k[x]$ 的素因子分解为

$$f(x)=ap_1(x)^{e_1}\cdots p_m(x)^{e_m},$$

其中 $a\in k$，对所有 i 有 $e_i\geq 1$，且 $p_1(x)$，…，$p_m(x)$ 是 $k[x]$ 中互异的首一不可约多项式．特别地，若 $f(x)$ 是 $k[x]$ 中一些线性因子的乘积，即，若 $f(x)$ 的所有根都在 k 中，则

$$f(x)=a(x-r_1)^{e_1}(x-r_2)^{e_2}\cdots(x-r_s)^{e_s},$$

其中对所有 j 有 $e_j\geq 1$．我们称 e_j 为根 r_j 的**重数**．因为域上的线性多项式总是不可约的，所以唯一因子分解表明根的重数是定义良好的．

这里有两个公式用来求 $k[x]$ 中两个多项式的最大公因子和最小公倍数．当考虑两个多项式时，我们允许在它们的素因子分解中指数 $e_i=0$，从而允许首一不可约多项式以相同的集合出现．

→ **命题 3.86** 设 k 是一个域，令 $g(x)=ap_1^{e_1}\cdots p_n^{e_n}\in k[x]$ 且 $h(x)=bp_1^{f_1}\cdots p_n^{f_n}\in k[x]$，其中 a，$b\in k$，p_i 是互异的首一不可约多项式，且对所有 i 有 e_i，$f_i\geq 0$．定义

$$m_i=\min\{e_i,f_i\} \quad 和 \quad M_i=\max\{e_i,f_i\}.$$ 277

则

$$(g,h)=p_1^{m_1}\cdots p_n^{m_n} \quad 和 \quad [g,h]=p_1^{M_1}\cdots p_n^{M_n}.$$

证明 改写命题 1.55 的证明即可．■

下面的结果与命题 1.47 类似：对 $b\geqslant 2$，每个正整数有一个以 b 为底数的展开式.

引理 3.87 设 k 是域，$b(x)\in k[x]$ 的次数为 $\deg(b)\geqslant 1$，则每个非零的 $f(x)\in k[x]$ 有展开式

$$f(x)=d_m(x)b(x)^m+\cdots+d_j(x)b(x)^j+\cdots+d_0(x),$$

其中对每个 j 有 $d_j(x)=0$ 或 $\deg(d_j)<\deg(b)$.

证明 根据除法算式，存在 $g(x)$，$d_0(x)\in k[x]$ 使得

$$f(x)=g(x)b(x)+d_0(x),$$

其中 $d_0(x)=0$ 或 $\deg(d_0)<\deg(b)$. 现在 $\deg(f)=\deg(gb)$，因为 $\deg(b)\geqslant 1$，所以 $\deg(g)<\deg(f)$. 根据归纳假设，存在 $d_j(x)\in k[x]$ 满足 $d_j(x)=0$ 或 $\deg(d_j)<\deg(b)$，并且

$$g(x)=d_m b^{m-1}+\cdots+d_2 b+d_1.$$

因此，

$$\begin{aligned}f&=gb+d_0\\&=(d_m b^{m-1}+\cdots+d_2 b+d_1)b+d_0\\&=d_m b^m+\cdots+d_2 b^2+d_1 b+d_0.\end{aligned}$$

■

像对整数一样，可以证明“数字”$d_i(x)$ 是唯一的(见命题 1.47).

定义 设 k 是域，多项式 $q_1(x)$，…，$q_n(x)\in k[x]$ 称为**两两互素**，若对所有 $i\neq j$ 有 $(q_i, q_j)=1$.

容易看出，若 $q_1(x)$，…，$q_m(x)$ 两两互素，则对所有 i 有 $q_i(x)$ 和 $q_1(x)\cdots\hat{q}_i(x)\cdots q_m(x)$ 互素.

引理 3.88 设 k 是一个域，$f(x)/g(x)\in k(x)$，并设 $g(x)=q_1(x)\cdots q_m(x)$，其中 $q_1(x)$，…，$q_m(x)\in k[x]$ 两两互素. 则存在 $a_i(x)\in k[x]$ 使得

278

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}\frac{a_i(x)}{q_i(x)}.$$

证明 对 $m\geqslant 1$ 用归纳法证明. 基础步骤 $m=1$ 显然成立. 由于 q_1 和 $q_2\cdots q_m$ 互素，所以存在多项式 s 和 t 使得 $1=sq_1+tq_2\cdots q_m$. 因此，

$$\begin{aligned}\frac{f}{g}&=(sq_1+tq_2\cdots q_m)\frac{f}{g}\\&=\frac{sq_1 f}{g}+\frac{tq_2\cdots q_m f}{g}\\&=\frac{sq_1 f}{q_1q_2\cdots q_m}+\frac{tq_2\cdots q_m f}{q_1q_2\cdots q_m}\\&=\frac{sf}{q_2\cdots q_m}+\frac{tf}{q_1}.\end{aligned}$$

因为 $q_2(x)$，…，$q_m(x)$ 两两互素，所以由归纳假设得证. ■

我们现在证明微积分中用部分分式积分有理函数的方法中的代数部分.

定理 3.89 (部分分式) 设 k 是域，首一多项式 $g(x)\in k[x]$ 的不可约因子分解为

$$g(x)=p_1(x)^{e_1}\cdots p_m(x)^{e_m}.$$

若 $f(x)/g(x)\in k(x)$，则

$$\frac{f(x)}{g(x)}=h(x)+\sum_{i=1}^{m}\left(\frac{d_{i1}(x)}{p_i(x)}+\frac{d_{i2}(x)}{p_i(x)^2}+\cdots+\frac{d_{ie_i}(x)}{p_i(x)^{e_i}}\right),$$

其中 $h(x)\in k[x]$，且 $d_{ij}(x)=0$ 或 $\deg(d_{ij})<\deg(p_i)$.

证明 显然，$p_1(x)^{e_1}$，$p_2(x)^{e_2}$，…，$p_m(x)^{e_m}$ 两两互素. 由引理 3.88 可知，存在 $a_i(x)\in k[x]$使得

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}\frac{a_i(x)}{p_i(x)^{e_i}}.$$

对每个 i，由除法算式得到多项式 $Q_i(x)$ 和 $R_i(x)$ 使得 $a_i(x)=Q_i(x)p_i(x)^{e_i}+R_i(x)$，其中 $R_i(x)=0$ 或 $\deg(R_i)<\deg(p_i(x)^{e_i})$. 因而

$$\frac{a_i(x)}{p_i(x)^{e_i}}=Q_i(x)+\frac{R_i(x)}{p_i(x)^{e_i}}.$$

由引理 3.87，

$$R_i(x)=d_{im}(x)p_i(x)^m+d_{i,m-1}(x)p_i(x)^{m-1}+\cdots+d_{i0}(x),$$ 279

其中对所有 j，$d_{ij}(x)=0$ 或 $\deg(d_{ij})<\deg(p_i)$. 而且由于 $\deg(R_i)<\deg(p_i^{e_i})$，所以 $m\leqslant e_i$. 因此，

$$\begin{aligned}\frac{a_i(x)}{p_i(x)^{e_i}}&=Q_i(x)+\frac{d_{im}(x)p_i(x)^m+d_{i,m-1}(x)p_i(x)^{m-1}+\cdots+d_{i0}(x)}{p_i(x)^{e_i}}\\&=Q_i(x)+\frac{d_{im}(x)p_i(x)^m}{p_i(x)^{e_i}}+\frac{d_{i,m-1}(x)p_i(x)^{m-1}}{p_i(x)^{e_i}}+\cdots+\frac{d_{i0}(x)}{p_i(x)^{e_i}}.\end{aligned}$$

消去后，每个被加数 $d_{ij}(x)p_i(x)^j/p_i(x)^{e_i}$ 或为多项式或为形如 $d_{ij}(x)/p_i(x)^s$ 的有理函数，其中 $1\leqslant s\leqslant e_i$. 若我们称 $h(x)$为所有这些不为有理函数的多项式的和，则这就是我们要证明的展开式. ■

我们已经知道，$\mathbb{R}[x]$中的不可约多项式只有线性多项式和二次多项式，所以$\mathbb{R}[x]$中部分分式分解中的所有分子或为常数或为线性多项式. 应用定理 3.89 可以证明$\mathbb{R}(x)$中的所有有理函数可以在闭型中积分.

这里有一个部分分式的整数模型. 若 a/b 是正有理数，其中 b 的素因子分解是 $b=p_1^{e_1}\cdots p_m^{e_m}$，则

$$\frac{a}{b}=h+\sum_{i=1}^{m}\left(\frac{c_{i1}}{p_i}+\frac{c_{i2}}{p_i^2}+\cdots+\frac{c_{ie_i}}{p_i^{e_i}}\right),$$

其中 $h\in\mathbb{Z}$ 且对所有 j，$0\leqslant c_{ij}<p_i$.

习题

H3.82 判断对错并说明理由.

(i)$\mathbb{Z}[x]$的每个元素是$\mathbb{Z}$中一个常数和$\mathbb{Z}[x]$中首一不可约多项式的积.

(ii)$\mathbb{Z}[x]$的每个元素是$\mathbb{Z}$中一个常数和$\mathbb{Q}[x]$中首一不可约多项式的积.

(iii)若 k 是一个域，$f(x)\in k[x]$既可以写成 $ap_1(x)\cdots p_m(x)$也可以写成 $bq_1(x)\cdots q_n(x)$，其中 a，b 是 k 中的常数，$p_1(x)$，…，$p_m(x)$都是首一不可约多项式，$q_1(x)$，…，$q_n(x)$都是首一非常数多项

式，则 $q_1(x)$，…，$q_n(x)$都是不可约的.

(iv)若 k 是一个域，$f(x)\in k[x]$既可以写成 $ap_1(x)\cdots p_m(x)$也可以写成 $bq_1(x)\cdots q_n(x)$，其中 a，b 是 k 中的常数，$p_1(x)$，…，$p_m(x)$都是首一不可约多项式，$q_1(x)$，…，$q_n(x)$都是首一非常数多项

280 式，则 $m\geqslant n$.

(v)若 k 是 K 的一个子域，$f(x)\in k[x]$有分解式 $f(x)=ap_1^{e_1}\cdots p_n^{e_n}$，其中 a 是一个常数，$p_i(x)$在$k[x]$中都是首一不可约的，则 $f(x)=ap_1^{e_1}\cdots p_n^{e_n}$ 也是 $f(x)$在 $K[x]$中分解为一个常数与一些首一不可约多项式乘积的表达式.

(vi)若 $f(x)$是域 K 上的多项式，$f(x)$在 $K[x]$中分解为一个常数与一些首一不可约多项式的乘积 $f(x)=ap_1^{e_1}\cdots p_n^{e_n}$. 若 $f(x)$和多项式 $p_i(x)$的所有系数都在某个子域 $k\subseteq K$ 中，则 $f(x)=ap_1^{e_1}\cdots p_n^{e_n}$ 也是 $f(x)$在 $k[x]$中分解为一个常数与一些首一不可约多项式乘积的表达式.

3.83 在 $k[x]$中，其中 k 为域，设 $g=p_1^{e_1}\cdots p_m^{e_m}$，$h=p_1^{f_1}\cdots p_m^{f_m}$，其中所有 p_i 是互异的首一不可约多项式，且对所有 i，e_i，$f_i\geqslant 0$. 证明 $g\mid h$ 当且仅当对所有 i 有 $e_i\leqslant f_i$.

*3.84 **H** (i)若 $f(x)\in\mathbb{R}[x]$，证明 $f(x)$在$\mathbb{C}$中没有重根当且仅当$(f,f')=1$.

(ii)证明，若 $p(x)\in\mathbb{Q}[x]$是一个不可约多项式，则 $p(x)$没有重根.

*3.85 设 $\zeta=e^{2\pi i/n}$.

H (i)证明

$$x^n-1=(x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}),$$

且若 n 是奇数，则

$$x^n+1=(x+1)(x+\zeta)(x+\zeta^2)\cdots(x+\zeta^{n-1}).$$

H (ii)对数 a，b，证明

$$a^n-b^n=(a-b)(a-\zeta b)(a-\zeta^2 b)\cdots(a-\zeta^{n-1}b),$$

且若 n 是奇数，则

$$a^n+b^n=(a+b)(a+\zeta b)(a+\zeta^2 b)\cdots(a+\zeta^{n-1}b).$$

→3.7 不可约性

尽管有一些方法可以帮助我们判断一个整数是否是素数，但解决一般问题却是很困难的，例如分解大的整数. 虽然判断一个多项式是否不可约也是很困难的，但我们现在提供一些有用的方法，它们是经常起作用的.

我们知道，若 $f(x)\in k[x]$，r 是 $f(x)$在域 k 中的一个根，则在 $k[x]$中存在一个分解 $f(x)=(x-r)g(x)$，这样 $f(x)$不是不可约的. 在推论 3.65 中，我们看到这个事实决定了 $k[x]$中二次和三次多项式的问题：这些多项式在 $k[x]$中不可约当且仅当它们在 k 中没有根. 另一方面，

281 可能存在这样的多项式，它没有根但不是不可约的，例如$(x^2+1)^2\in\mathbb{R}[x]$.

→ **定理 3.90** 设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$. 则 $f(x)$的每个有理根有形式 $r=b/c$，其中$b\mid a_0$，$c\mid a_n$.

证明 我们可以假设 $r=b/c$ 是既约形式，即$(b,c)=1$. 把 r 代入 $f(x)$得

$$0=f(b/c)=a_0+a_1b/c+\cdots+a_nb^n/c^n,$$

乘以 c^n 得

$$0=a_0c^n+a_1bc^{n-1}+\cdots+a_nb^n.$$

因而，$a_0c^n=b(-a_1c^{n-1}-\cdots-a_nb^{n-1})$，即，$b\mid a_0c^n$. 因为 b 与 c 互素，所以 b 与 c^n 互素，由推论 1.40 以及欧几里得引理知 $b\mid a_0$. 类似地，$a_nb^n=c(-a_{n-1}b^{n-1}-\cdots-a_0c^{n-1})$，$c\mid a_nb^n$，$c\mid a_n$. ■

定义 复数 α 称为**代数整数**，若 α 是首一多项式 $f(x)\in\mathbb{Z}[x]$的一个根.

我们注意到，在代数整数的定义中，要求 $f(x)\in\mathbb{Z}[x]$是首一的是很关键的. 每个代数数 β，即每个复数 β 是某个多项式 $g(x)\in\mathbb{Q}[x]$的根，必定是某个多项式 $h(x)\in\mathbb{Z}[x]$的根，只要把 $g(x)$的系数的分母清除即可.

推论 3.91 若代数整数 α 是有理数，则必有 $\alpha\in\mathbb{Z}$. 准确地说，若 $f(x)\in\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$是首一多项式，则 $f(x)$的每个有理根是一个能整除常数项的整数.

证明 若 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 是首一的，则 $a_n=1$，可以马上运用定理 3.90 得证. ■

例如，考虑 $f(x)=x^3+4x^2-2x-1\in\mathbb{Q}[x]$. 根据推论 3.65，这个三次多项式是不可约的当且仅当它没有有理根. 因为 $f(x)$是首一的，所以有理根只能是 ±1，因为它们是 -1 在$\mathbb{Z}$中仅有的因子. 但是 $f(1)=2$，$f(-1)=4$，所以 1 和 -1 都不是根. 因此 $f(x)$在$\mathbb{Q}$ 中没有根，因而 $f(x)$在$\mathbb{Q}[x]$中是不可约的.

推论 3.91 给出了习题 1.70 的一个新的解法. 若 m 是整数但不是完全平方数，则多项式 x^2-m 没有整数根，因而$\sqrt{m}$是无理数. 事实上，读者现在可推广到 n 次方根：若 m 不是一个整数的 n 次幂，则$\sqrt[n]{m}$是无理数，因为 x^n-m 的任意有理根都必须是整数.

我们将寻找几个条件，这些条件能推出多项式 $f(x)\in\mathbb{Z}[x]$在$\mathbb{Z}[x]$中不能分解为更小次数的多项式的乘积. 因为$\mathbb{Z}$ 不是域，所以这不能说明 $f(x)$在$\mathbb{Z}[x]$中是不可约的. 例如，$f(x)=2x+2$ 在$\mathbb{Z}[x]$中不能这样分解，但它不是不可约的. 然而，高斯证明了：若 $f(x)\in\mathbb{Z}[x]$在$\mathbb{Z}[x]$中不能分解为更小次数的多项式的乘积，则 $f(x)$在$\mathbb{Q}[x]$中是不可约的. 我们先证明几个引理，然后证明这个结果. 282

→ **定义** 多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in\mathbb{Z}[x]$称为**本原的**，若它的系数的最大公因子是 1.

当然，每个首一多项式都是本原的. 容易看出，若 d 是 $f(x)$的系数的最大公因子，则 $(1/d)f(x)$是$\mathbb{Z}[x]$中的本原多项式.

→ **引理 3.92（高斯引理）** 若 $f(x)$，$g(x)\in\mathbb{Z}[x]$都是本原的，则它们的乘积 $f(x)g(x)$也是本原的.

证明 设 $f(x)=\sum a_ix^i$，$g(x)=\sum b_jx^j$，$f(x)g(x)=\sum c_kx^k$. 若 $f(x)g(x)$不是本原的，则存在素数 p 整除每个 c_k. 由于 $f(x)$是本原的，所以它至少有一个系数不能被 p 整除，设 a_i 是第一个这样的系数. 类似地，设 b_j 是 $g(x)$的第一个不能被 p 整除的系数. 由多项式乘法的定义得

$$a_ib_j=c_{i+j}-(a_0b_{i+j}+\cdots+a_{i-1}b_{j+1}+a_{i+1}b_{j-1}+\cdots+a_{i+j}b_0).$$

右边每一项都被 p 整除，所以 p 整除 a_ib_j. 但是 p 既不整除 a_i 也不整除 b_j，这就与$\mathbb{Z}$ 中的欧几里得引理矛盾. ■

最后一个引理有一个更漂亮的证法. 若多项式 $h(x)\in\mathbb{Z}[x]$不是本原的，则存在素数 p 可整除它的每一个系数(若所有系数的最大公因子是 $d>1$，则取 p 为 d 的素因子). 既然这样，$h(x)$的所有系数在$\mathbb{F}_p$ 中都为 0. 若 $\varphi:\mathbb{Z}\to\mathbb{F}_p$ 是自然映射 $a\mapsto[a]$，则由定理 3.33 知，函数 $\varphi^*:\mathbb{Z}[x]\to\mathbb{F}_p[x]$是一个环同态. 假设本原多项式的乘积 $f(x)g(x)$不是本原的，则在$\mathbb{F}_p[x]$中 $0=\varphi^*(fg)=\varphi^*(f)\varphi^*(g)$. 另一方面，$\varphi^*(f)$和 $\varphi^*(g)$都不为 0，因为它们都是本原的. 这就与$\mathbb{F}_p[x]$是整环的事实矛盾.

→ **引理 3.93** 每个非零的 $f(x)\in\mathbb{Q}[x]$都有唯一的因子分解

$$f(x)=c(f)f^{\#}(x),$$

283 其中 $c(f)\in\mathbb{Q}$ 是正数，$f^{\#}(x)\in\mathbb{Z}[x]$是本原的.

证明 存在整数 a_i 和 b_i 使得

$$f(x)=(a_0/b_0)+(a_1/b_1)x+\cdots+(a_n/b_n)x^n\in\mathbb{Q}[x].$$

定义 $B=b_0b_1\cdots b_n$，使得 $g(x)=Bf(x)\in\mathbb{Z}[x]$. 现在定义 $D=\pm d$，其中 d 是 $g(x)$的所有系数的最大公因子，选取符号使得有理数 D/B 为正. 现在$(B/D)f(x)=(1/D)g(x)\in\mathbb{Z}[x]$，且是一个本原多项式. 若我们定义 $c(f)=D/B$ 和 $f^{\#}(x)=(B/D)f(x)$，则 $f(x)=c(f)f^{\#}(x)$是要证的因子分解.

假设 $f(x)=eh(x)$是另一个这样的因子分解，则 e 是正有理数，$h(x)\in\mathbb{Z}[x]$是本原的. 现在 $c(f)f^{\#}(x)=f(x)=eh(x)$，所以 $f^{\#}(x)=[e/c(f)]h(x)$. 记 $e/c(f)$为既约形式：$e/c(f)=u/v$，其中 u 和 v 是互素的正整数. 等式 $vf^{\#}(x)=uh(x)$在$\mathbb{Z}[x]$中成立，则 v 是 $uh(x)$的每个系数的公因子. 因为$(u,v)=1$，所以由$\mathbb{Z}$ 中欧几里得引理知 v 是 $h(x)$的系数的(正)公因子. 由于 $h(x)$是本原的，于是 $v=1$. 类似的讨论可证明 $u=1$. 由于 $e/c(f)=u/v=1$，所以 $e=c(f)$，因而 $h(x)=f^{\#}(x)$. ■

→ **定义** 引理 3.93 中的有理数 $c(f)$称为 $f(x)$的**容度**.

推论 3.94 若 $f(x)\in\mathbb{Z}[x]$，则 $c(f)\in\mathbb{Z}$.

证明 若 d 是 $f(x)$的系数的最大公因子，则$(1/d)f(x)\in\mathbb{Z}[x]$是本原的. 因为 $d[(1/d)f(x)]$是 $f(x)$的一个因子分解，是一个正有理数 d (甚至是一个正整数)和一个本原多项式的乘积，所以由引理 3.93 中的唯一性知 $c(f)=d\in\mathbb{Z}$. ■

推论 3.95 若 $f(x)\in\mathbb{Q}[x]$可分解为 $f(x)=g(x)h(x)$，则

$$c(f)=c(g)c(h)\quad\text{和}\quad f^{\#}(x)=g^{\#}(x)h^{\#}(x).$$

证明 我们有

$$\begin{aligned}f(x)&=g(x)h(x)\\c(f)f^{\#}(x)&=[c(g)g^{\#}(x)][c(h)h^{\#}(x)]\\&=c(g)c(h)g^{\#}(x)h^{\#}(x).\end{aligned}$$

由引理 3.92 知 $g^{\#}(x)h^{\#}(x)$是本原的，又因为 $c(g)c(h)$是正有理数，所以由引理 3.93 中因子
284 分解的唯一性知 $c(f)=c(g)c(h)$，$f^{\#}(x)=g^{\#}(x)h^{\#}(x)$. ■

→ **定理 3.96(高斯)** 设 $f(x)\in\mathbb{Z}[x]$. 若在$\mathbb{Q}[x]$中

$$f(x)=G(x)H(x),$$

则在$\mathbb{Z}[x]$中存在因子分解

$$f(x)=g(x)h(x),$$

其中 $\deg(g)=\deg(G)$，$\deg(h)=\deg(H)$. 因此，若 $f(x)$不能在$\mathbb{Z}[x]$中分解为更低次的多项式的乘积，则 $f(x)$在$\mathbb{Q}[x]$中是不可约的.

证明 根据推论 3.95，在$\mathbb{Q}[x]$中存在因子分解

$$f(x)=c(G)c(H)G^{\#}(x)H^{\#}(x),$$

其中 $G^{\#}(x)$，$H^{\#}(x)\in\mathbb{Z}[x]$是本原多项式. 但是，由推论 3.95 知 $c(G)c(H)=c(f)$，又由推论 3.94(应用它是因为 $f(x)\in\mathbb{Z}[x]$)知 $c(f)\in\mathbb{Z}$. 因此，$f(x)=g(x)h(x)$是$\mathbb{Z}[x]$中的因子分解，其中 $g(x)=c(f)G^{\#}(x)$，$h(x)=H^{\#}(x)$. ■

注 高斯利用这些思想证明了定理 7.21：系数在域 k 中的所有 n 元多项式构成的环 $k[x_1,\cdots,x_n]$是一个唯一因子分解整环.

→ **定理 3.97** 设 $f(x)=a_0+a_1x+a_2x^2+\cdots+x^n\in\mathbb{Z}[x]$是首一的，并设 p 是素数. 若 $f^*(x)=[a_0]+[a_1]x+[a_2]x^2+\cdots+x^n$ 在$\mathbb{F}_p[x]$中是不可约的，则 $f(x)$在$\mathbb{Q}[x]$中是不可约的.

证明 根据定理 3.33，自然映射 $\varphi:\mathbb{Z}\to\mathbb{F}_p$ 定义一个同态 $\varphi^*:\mathbb{Z}[x]\to\mathbb{F}_p[x]$为

$$\varphi^*(b_0+b_1x+b_2x^2+\cdots)=[b_0]+[b_1]x+[b_2]x^2+\cdots.$$

若 $g(x)\in\mathbb{Z}[x]$，则记它的象 $\varphi^*(g(x))\in\mathbb{F}_p[x]$为 $g^*(x)$. 假设 $f(x)$在$\mathbb{Z}[x]$中可分解，不妨设为 $f(x)=g(x)h(x)$，其中 $\deg(g)<\deg(f)$，$\deg(h)<\deg(f)$[当然，$\deg(f)=\deg(g)+\deg(h)$]. 因为 φ^* 是环同态，所以 $f^*(x)=g^*(x)h^*(x)$，所以 $\deg(f^*)=\deg(g^*)+\deg(h^*)$. 由于 $f(x)$是首一的，所以 $f^*(x)$也是首一的，所以 $\deg(f^*)=\deg(f)$. 因此，$g^*(x)$和 $h^*(x)$的次数都小于 $\deg(f^*)$，这与 $f^*(x)$的不可约性矛盾. 因此，$f(x)$在$\mathbb{Z}[x]$中是不可约的，由高斯定理知 $f(x)$在$\mathbb{Q}[x]$中是不可约的. ■ 285

定理 3.97 的逆命题不成立，另外它也不是一直奏效的. 不难求出一个多项式$f(x)\in\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$是不可约的，但对某个素数 p 有 $f^*(x)\in\mathbb{F}_p[x]$是可分解的. 根据习题 3.100，x^4+1 在$\mathbb{Q}[x]$中是不可约的，但它在$\mathbb{F}_p[x]$中可分解，其中 p 是任意素数.

定理 3.97 是说，若我们可以找到一个素数 p 使得 $f^*(x)$在$\mathbb{F}_p[x]$中是不可约的，则 $f(x)$在$\mathbb{Q}[x]$中是不可约的. 直到现在，有限域$\mathbb{F}_p$ 还是令人奇怪的. 因为在$\mathbb{F}_p[x]$中任意固定次数的多项式只有有限多个，所以$\mathbb{F}_p$ 的有限性是一个很大的优势. 原则上，我们可以通过观察 n 次多项式的所有可能的因子分解来判断它在$\mathbb{F}_p[x]$中是否是不可约的.

为方便起见，我们现在写$\mathbb{F}_p$ 的元素时不再用中括号.

例 3.98 我们确定$\mathbb{F}_2[x]$中次数较小的不可约多项式.

和以往一样，线性多项式 x 和 $x+1$ 都是不可约的.

二次多项式有四个：x^2，x^2+x，x^2+1，x^2+x+1（一般地，在$\mathbb{F}_p[x]$中 n 次首一多项式有 p^n 个，这是因为 n 个系数 $a_0,\cdots,a_{n-1}$ 中的每一个都有 p 种选法）. 因为前面三个都在$\mathbb{F}_2$ 中有根，所以仅有一个不可约的二次多项式.

三次多项式有八个，其中有四个是可约的，这是因为它们的常数项都是 0. 剩下的多项

式是

$$x^3+1, x^3+x+1, x^3+x^2+1, x^3+x^2+x+1.$$

由于 1 是第一和第四个的根，所以只有中间两个是不可约的三次多项式.

四次多项式有 16 个，其中八个是可约的，这是因为它们的常数项都是 0. 常数项不为 0 的那八个中，非零系数为偶数个的多项式有一个根为 1. 现在只剩下四个多项式 $f(x)$，且它们中的每一个在 $\mathbb{F}_2$ 中都没有根，即它们都没有线性因子. 若 $f(x)=g(x)h(x)$，则 $g(x)$ 和 $h(x)$ 都一定是不可约的二次多项式. 但是只有一个不可约的二次多项式 x^2+x+1，所以 $(x^2+x+1)^2=x^4+x^2+1$ 是可约的，而其他三个都是不可约的. 下列表格概括了这些观察结果.

$\mathbb{F}_2$ 中低次数的不可约多项式

2 次：x^2+x+1.

3 次：x^3+x+1，x^3+x^2+1.

286 4 次：x^4+x^3+1，x^4+x+1，$x^4+x^3+x^2+x+1$. ◀

例 3.99 以下是 $\mathbb{F}_3[x]$ 中首一不可约的二次和三次多项式的一个列表. 读者可以通过计算所有这些多项式来验证这个列表是对的. 常数项不为零的首一的二次多项式有 6 个，常数项不为零的首一的三次多项式有 18 个. 然后检验这些多项式中哪些是以 1 或 -1 为根的(用 -1 代替 2 会更方便些).

$\mathbb{F}_3$ 中首一的不可约二次和三次多项式

2 次：	x^2+1,	x^2+x-1,	x^2-x-1.
3 次：	x^3-x+1,	x^3+x^2-x+1,	x^3-x^2+1,
	x^3-x^2+x+1,	x^3+x^2-1,	x^3-x^2-1,
	x^3+x^2+x-1,	x^3-x^2-x-1.	

◀

例 3.100 (i)我们证明 $f(x)=x^4-5x^3+2x+3$ 在 $\mathbb{Q}[x]$ 中是不可约多项式. 根据推论 3.91，$f(x)$ 的有理根只可能是 1，-1，3，-3，读者可以检验它们都不是根. 由于 $f(x)$ 是四次多项式，所以我们还不能断言 $f(x)$ 是不可约的，因为它可能是(不可约的)二次多项式的乘积.

让我们试一下定理 3.97 中的准则. 因为 $f^*(x)=x^4+x^3+1$ 在 $\mathbb{F}_2[x]$ 中不可约，所以根据例 3.98，$f(x)$ 在 $\mathbb{Q}[x]$ 中不可约. [不必检验 $f(x)$ 没有有理根，$f^*(x)$ 的不可约性足够得出 $f(x)$ 的不可约性.]

(ii)设 $\Phi_5(x)=x^4+x^3+x^2+x+1\in\mathbb{Q}[x]$. 在例 3.98 中，我们看到 $(\Phi_5)^*(x)=x^4+x^3+x^2+x+1$ 在 $\mathbb{F}_2[x]$ 中不可约，所以 $\Phi_5(x)$ 在 $\mathbb{Q}[x]$ 中不可约. ◀

因为任意线性多项式在 $\mathbb{Q}[x]$ 中不可约，所以 $\Phi_2(x)=x+1$ 在 $\mathbb{Q}[x]$ 中不可约. $\Phi_3(x)=x^2+x+1$ 在 $\mathbb{Q}[x]$ 中不可约，因为它没有有理根. 我们刚才看到 $\Phi_5(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 让我们引入另一个不可约准则来证明：对所有素数 p，$\Phi_p(x)$ 在 $\mathbb{Q}[x]$ 中是不可约的.

引理 3.101 *设 $g(x)\in\mathbb{Z}[x]$. 若存在 $c\in\mathbb{Z}$ 使得 $g(x+c)$ 在 $\mathbb{Z}[x]$ 中不可约，则 $g(x)$ 在 $\mathbb{Q}[x]$ 中不可约.*

证明 根据定理 3.33，函数 $\varphi:\mathbb{Z}[x]\to\mathbb{Z}[x]$，$f(x)\mapsto f(x+c)$ 是一个同构. 假设 $g(x)=$

$s(x)t(x)$，则 $g(x+c)=\varphi(g(x))=\varphi(st)=\varphi(s)\varphi(t)$，此与 $g(x+c)$ 在 $\mathbb{Z}[x]$ 中不可约矛盾．因此，$g(x)$ 在 $\mathbb{Z}[x]$ 中不可约，因而根据高斯定理，$g(x)$ 在 $\mathbb{Q}[x]$ 中不可约． ■ 287

→ **定理 3.102（艾森斯坦因准则）** 设 $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$．若存在素数 p，对所有 $i<n$ 有 $p\mid a_i$，但 $p\nmid a_n$，$p^2\nmid a_0$，则 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

证明 假设

$$f(x)=(b_0+b_1x+\cdots+b_mx^m)(c_0+c_1x+\cdots+c_kx^k),$$

其中 $m<n$，$k<n$．根据定理 3.96，我们可以假设这两个因子都在 $\mathbb{Z}[x]$ 中．现在 $p\mid a_0=b_0c_0$，所以由 $\mathbb{Z}$ 中欧几里得引理知 $p\mid b_0$ 或 $p\mid c_0$．由于 $p^2\nmid a_0$，所以 b_0，c_0 中只有一个可以被 p 整除，不妨设 $p\mid c_0$，$p\nmid b_0$．根据题设，首项系数 $a_n=b_mc_k$ 不能被 p 整除，所以 p 不整除 c_k（或 b_m）．设 c_r 是第一个不能被 p 整除的系数（所以 p 整除 c_0，…，c_{r-1}）．假设 $r<n$，则 $p\mid a_r$，所以 $b_0c_r=a_r-(b_1c_{r-1}+\cdots+b_rc_0)$ 也被 p 整除．$p\mid b_0c_r$ 而 p 不能整除这两个因子，这与欧几里得引理矛盾．于是 $r=n$，因而 $n\geqslant k\geqslant r=n$，所以 $k=n$，此与 $k<n$ 矛盾．因此 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约． ■

注 辛格（R. Singer）给出了艾森斯坦因（Eisenstein）准则的一个精彩的证明．

设 $\varphi^*:\mathbb{Z}[x]\to\mathbb{F}_p[x]$ 是环同态，$\varphi^*(f(x))$ 用 $f^*(x)$ 表示．若 $f(x)$ 在 $\mathbb{Q}[x]$ 中不是不可约的，则由高斯定理知存在多项式 $g(x)$，$h(x)\in\mathbb{Z}[x]$ 使得 $f(x)=g(x)h(x)$，其中 $g(x)=b_0+b_1x+\cdots+b_mx^m$，$h(x)=c_0+c_1x+\cdots+c_kx^k$，$m$，$k>0$．因此，在 $\mathbb{F}_p[x]$ 中有等式 $f^*(x)=g^*(x)h^*(x)$．

由于 $p\nmid a_n$，所以 $f^*(x)\neq 0$．实际上，存在某个单位 $u\in\mathbb{F}_p$ 使得 $f^*(x)=ux^n$，这是因为除首项系数之外其他所有系数都为 0．根据定理 3.84，$\mathbb{F}_p[x]$ 内的唯一因子分解，我们必有 $g^*(x)=vx^m$，$h^*(x)=wx^k$，其中 v，w 是 $\mathbb{F}_p$ 的单位，这是因为 x^n 的首一因子是 x 的幂．于是 $g^*(x)$ 和 $h^*(x)$ 的常数项都是 0，即 $\mathbb{F}_p$ 中 $[b_0]=0=[c_0]$，等价地，$p\mid b_0$，$p\mid c_0$．但是 $a_0=b_0c_0$，所以 $p^2\mid a_0$，矛盾．因此 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

回顾一下 $x^n-1=\prod_{d\mid n}\Phi_d(x)$，其中 $n\geqslant 1$，$\Phi_d(x)$ 是 d 次分圆多项式（在命题 3.47 中，我们已经证明了对所有 $d\geqslant 1$ 有 $\Phi_d(x)\in\mathbb{Z}[x]$）．特别地，若 $n=p$ 是素数，则

$$\Phi_p(x)=(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

→ **推论 3.103（高斯）** 对每个素数 p，p 次分圆多项式 $\Phi_p(x)$ 在 $\mathbb{Q}[x]$ 中不可约．

注 对任意 $d\geqslant 1$（不必是素数），分圆多项式 $\Phi_d(x)$ 在 $\mathbb{Q}[x]$ 中不可约（见缇格诺（Tignol）编写的《代数方程的伽罗瓦理论》（Galois' Theory of Algebraic Equations）中的定理 12.31）． 288

证明 由于 $\Phi_p(x)=(x^p-1)/(x-1)$，所以

$$\begin{aligned}\Phi_p(x+1)&=[(x+1)^p-1]/x\\&=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\cdots+p.\end{aligned}$$

由于 p 是素数，由命题 1.39 知，可以应用艾森斯坦因准则，我们得出 $\Phi_p(x+1)$ 在 $\mathbb{Q}[x]$ 中不

可约的结论．根据引理 3.101，$\Phi_p(x)$在$\mathbb{Q}[x]$中不可约． ■

我们没有说当 n 不是素数时 $x^{n-1}+x^{n-2}+\cdots+x+1$ 是不可约的．例如，当 $n=4$ 时，$x^3+x^2+x+1=(x+1)(x^2+1)$．

习题

H 3.86 判断对错并说明理由．

(i)$\sqrt{3}$是一个代数整数．

(ii)$\frac{13}{78}$是 $1+5x+6x^2$ 的一个有理根．

(iii)若 $f(x)=3x^4+ax^3+bx^2+cx+7$，其中 a，b，$c\in\mathbb{Z}$，则 $f(x)$在$\mathbb{Q}$中的根（如果有的话）在$\left\{\pm1，\pm7，\pm\frac{1}{3}，\pm\frac{7}{3}\right\}$中．

(iv)若 $f(x)=3x^4+ax^3+bx^2+cx+7$，其中 a，b，$c\in\mathbb{Q}$，则 $f(x)$在$\mathbb{Q}$中的根（如果有的话）在$\left\{\pm1，\pm7，\pm\frac{1}{3}，\pm\frac{7}{3}\right\}$中．

(v)$6x^2+10x+15$ 是一个本原多项式．

(vi)$\mathbb{Z}[x]$中的每个本原多项式是不可约的．

(vii)$\mathbb{Z}[x]$中每个不可约多项式是本原多项式．

(viii)$\mathbb{Z}[x]$中每个首一多项式是本原多项式．

(ix)$3x+\frac{1}{5}$的容度是$\frac{3}{5}$．

(x)$3x+\frac{6}{5}$的容度是$\frac{3}{5}$．

(xi)若$\mathbb{Q}[x]$中 $f(x)=g(x)h(x)$，且 $f(x)$的所有系数在$\mathbb{Z}$中，则 $g(x)$和 $h(x)$的所有系数也在$\mathbb{Z}$中．

(xii)对每个整数 c，多项式$(x+c)^2-(x+c)-1$ 在$\mathbb{Q}[x]$中不可约．

(xiii)对所有整数 n，多项式 x^8+5x^3+5n 在$\mathbb{Q}[x]$中不可约．

(xiv)对每个整数 n，多项式 $x^7+9x^3+(9n+6)$在$\mathbb{Q}[x]$中不可约．

***H 3.87** 确定下述多项式是否在$\mathbb{Q}[x]$中不可约．

(i) $f(x)=3x^2-7x-5$．

(ii) $f(x)=350x^3-25x^2+34x+1$．

(iii) $f(x)=2x^3-x-6$．

(iv) $f(x)=8x^3-6x-1$．

(v) $f(x)=x^3+6x^2+5x+25$．

(vi) $f(x)=x^5-4x+2$．

289 (vii) $f(x)=x^4+x^2+x+1$．

(viii) $f(x)=x^4-10x^2+1$．

(ix) $f(x)=x^6-210x-616$．

(x) $f(x)=350x^3+x^2+4x+1$．

3.88 若 p 是一个素数，证明$\mathbb{F}_p[x]$中恰有$\frac{1}{3}(p^3-p)$个首一不可约三次多项式．

H 3.89　证明$\mathbb{F}_2[x]$中恰有 6 个不可约五次多项式.

3.90　H (i)若 $a\neq\pm1$ 是一个非平方整数，证明对每个 $n\geqslant1$，x^n-a 在$\mathbb{Q}[x]$中不可约. 由此得到，对每个次数 $n\geqslant1$，$\mathbb{Q}[x]$中有不可约多项式.

(ii)若 $a\neq\pm1$ 是一个非平方整数，证明$\sqrt[n]{a}$是无理数.

H 3.91　设 k 是一个域，$f(x)=a_0+a_1x+\cdots+a_nx^n\in k[x]$的次数为 n. 若 $f(x)$是不可约的，则 $a_n+a_{n-1}x+\cdots+a_0x^n$ 也是不可约的.

→3.8　商环与有限域

代数基本定理是说，每个非常数多项式 $f(x)\in\mathbb{C}[x]$的所有根都在$\mathbb{C}$中(具体地讲，$f(x)$是$\mathbb{C}[x]$中一些线性多项式的积). 我们现在回到理想和同态上来，目的是证明任意域 k 上的多项式满足一个“部分”类似于代数基本定理的命题：给定多项式 $f(x)\in k[x]$，则存在某个域 K，它包含 k 且含有 $f(x)$的所有根. 我们称之为部分类似，是因为即使 K 含有多项式$f(x)$的所有根，它也可能不含有 $k[x]$中其他多项式的所有根. 构造 K 的主要思想涉及商环的概念，是构造 $\mathbb{I}_m$ 的一个直接推广.

给定$\mathbb{Z}$和整数 m，定义$\mathbb{Z}$上的同余关系为：

$$a\equiv b \bmod m \quad \text{当且仅当} \quad m\mid(a-b).$$

该定义可以写为：$a\equiv b \bmod m$ 当且仅当$a-b\in(m)$，其中(m)表示$\mathbb{Z}$中由 m 生成的主理想. 该同余是$\mathbb{Z}$上的一个等价关系，其等价类$[a]$叫做同余类，集合$\mathbb{I}_m$ 是所有同余类构成的族.

我们现在进行一个新的构造. 给定交换环 R 和理想 I，定义 R 上的一个叫做**同余** mod I 的关系：

$$a\equiv b \bmod I \quad \text{当且仅当} \quad a-b\in I.$$

→ **引理 3.104**　*若 R 是交换环，I 是 R 中的理想，则同余 mod I 是 R 上的一个等价关系.*

证明　(i)自反性：若 $a\in R$，则 $a-a=0\in I$，因此 $a\equiv a \bmod I$. 290

(ii)对称性：若 $a\equiv b \bmod I$，则 $a-b\in I$. 因为$-1\in R$，所以 $b-a=(-1)(a-b)\in I$，这样 $b\equiv a \bmod I$.

(iii)传递性：若 $a\equiv b \bmod I$，$b\equiv c \bmod I$，则 $a-b\in I$，$b-c\in I$. 因此 $a-c=(a-b)+(b-c)\in I$，$a\equiv c \bmod I$. ■

→ **定义**　*若 R 是交换环，I 是 R 中的理想，则称 $a\in R$ 的等价类$[a]=\{b\in R: b\equiv a \bmod I\}$为 a mod I 的***同余类***. 所有同余类构成的集合记为 R/I：*

$$R/I=\{[a]: a\in R\}.$$

我们记得$\mathbb{I}_m$ 上的加法和乘法是由下列两个公式定义的：

$$[a]+[b]=[a+b] \quad \text{和} \quad [a][b]=[ab].$$

这些函数 $\mathbb{I}_m\times\mathbb{I}_m\to\mathbb{I}_m$ 是否定义良好是不显然的，我们不得不证明它们是定义良好的(见命题 2.103和命题 2.105). 这些公式也给出了 R/I 上的加法和乘法运算.

引理 3.105　*函数*

$$\alpha:(R/I)\times(R/I)\to R/I, \quad ([a],[b])\mapsto[a+b],$$

和

$$\mu:(R/I)\times(R/I)\to R/I,\quad ([a],[b])\mapsto[ab]$$

是 R/I 上定义良好的两个运算.

证明 让我们证明 α 和 μ 是定义良好的. 回忆引理 2.19：若 $\equiv$ 是集合 X 上的一个等价关系，则 $[a]=[a']$ 当且仅当 $a\equiv a'$，在这里，$[a]=[a']$ 当且仅当 $a-a'\in I$. 加法是否定义良好? 即，若 $[a]=[a']$，$[b]=[b']$，则 $[a+b]=[a'+b']$ 是否成立? 即，若 $a-a'\in I$，$b-b'\in I$，则 $(a+b)-(a'+b')\in I$ 是否成立? 答案是肯定的，因为 $(a+b)-(a'+b')=(a-a')+(b-b')\in I$. 因此 $[a+b]=[a'+b']$. 乘法是否定义良好? 即，若 $[a]=[a']$，$[b]=[b']$，则 $[ab]=[a'b']$ 是否成立? 现在 $a-a'\in I$，$b-b'\in I$，所以

$$ab-a'b'=(ab-ab')+(ab'-a'b')=a(b-b')+(a-a')b'\in I.$$

因此 $[ab]=[a'b']$. ■

R/I 带上引理 3.105 中的两个运算是一个交换环的证明与 $\mathbb{I}_m$ 是交换环的证明是完全相同的. 从本质上讲，R/I 中的环公理成立是因为它们继承了 R 中的环公理. 291

→ **定理 3.106** *若 I 是交换环 R 中的理想，则 R/I 带上引理 3.105 中定义的加法和乘法运算是一个交换环.*

证明 我们验证交换环定义中的每个公理.

(i)因为在 R 中有 $a+b=b+a$，所以

$$[a]+[b]=[a+b]=[b+a]=[b]+[a].$$

(ii)因为 $[a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]$，$([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]$，又因为 $a+(b+c)=(a+b)+c$，所以 $[a]+([b]+[c])=([a]+[b])+[c]$.

(iii)定义 $0=[0]$，其中，括号中的 0 是 R 中的零元素. 因为在 R 中有 $0+a=a$，所以 $0+[a]=[0+a]=[a]$.

(iv)定义 $[a]'=[-a]$，现在 $[-a]+[a]=[-a+a]=[0]=0$.

(v)因为在 R 中有 $ab=ba$，所以 $[a][b]=[ab]=[ba]=[b][a]$.

(vi)因为 $[a]([b][c])=[a][bc]=[a(bc)]$，$([a][b])[c]=[ab][c]=[(ab)c]$，又因为 $(ab)c=a(bc)$，所以 $[a]([b][c])=([a][b])[c]$.

(vii)定义 $1=[1]$，其中，括号中的 1 是 R 中的单位元. 因为在 R 中有 $1a=a$，所以 $1[a]=[1a]=[a]$.

(viii)我们利用 R 中的分配律：$[a]([b]+[c])=[a][b+c]=[a(b+c)]$，$[a][b]+[a][c]=[ab]+[ac]=[ac+ab]=[a(b+c)]$. ■

→ **定义** *交换环 R/I 称为 R mod I 的***商环**.

$\mathbb{I}_m$ 中，同余类 $[a]=\{b\in\mathbb{Z}:b=a+km,\ k\in\mathbb{Z}\}$ 可以被描述为陪集 $[a]=a+(m)$，并且该描述可以推广到商环的元素上来.

→ **定义** *设 R 是一个交换环，I 是一个理想，则 R 的形如*

$$a+I=\{b\in R:b=a+i,i\in I\}$$

*的子集称为***陪集**.

我们现在证明陪集与同余类是相同的.

→ **引理 3.107** 设 R 是一个交换环，I 是一个理想，则在 R/I 中同余类$[a]$就是陪集 $a+I$.

证明 若 $b\in[a]$，则 $b-a\in I$. 因此 $b=a+(b-a)\in a+I$，这样$[a]\subseteq a+I$. 对于反包含，若 $c\in a+I$，则存在 $i\in I$ 使得 $c=a+i$，因此 $c-a\in I$，$c\equiv a \bmod I$，$c\in[a]$，$a+I\subseteq[a]$. 这样$[a]=a+I$. ■

陪集记号 $a+I$ 是使用非常普遍的记号，这样

$$R/I=\{a+I: a\in R\}.$$ 292

注 若我们忽略交换环 R 中的乘法运算，则 R 是一个加法阿贝尔群，并且 R 中的每个理想是一个子群. 因为阿贝尔群的子群是正规子群，所以商群 R/I 是可以定义的. 我们声称该商群与商环 R/I 的加法群是一致的. 每个群的元素相同(它们是 I 的陪集)，并且在每个群中陪集的加法也相同. 特别地，$\mathbb{Z}$ 中的主理想(m)记为 $m\mathbb{Z}$，并且我们已经把商环$\mathbb{Z}/m\mathbb{Z}$ 记为$\mathbb{I}_m$ 了.

→ **定义** 设 R 是一个交换环，I 是一个理想，则由 $\pi(a)=a+I$ 定义的 $\pi: R\to R/I$ 称为**自然映射**.

让我们证明 $\pi: R\to R/I$ 是一个同态. 首先 $\pi(1)=1+I$ 是 R/I 中的单位元. 由 R/I 中加法的定义知

$$\pi(a)+\pi(b)=(a+I)+(b+I)=a+b+I=\pi(a+b).$$

由乘法的定义知

$$\pi(a)\pi(b)=(a+I)(b+I)=ab+I=\pi(ab).$$

我们现在证明命题 3.38 的逆命题.

→ **命题 3.108** 交换环 R 中的每个理想 I 是某个同态的核. 具体来讲，自然映射 $\pi: R\to R/I$ 是一个满同态，且它的核是 I.

证明 R/I 的元素是陪集 $a+I$. 因为 $a+I=\pi(a)$，所以自然映射是满的. 因为若 $a\in I$ 则 $\pi(a)=a+I=0+I$，所以 $I\subseteq\ker\pi$. 对于反包含，若 $a\in\ker\pi$，则 $\pi(a)=a+I=I$，这样 $a\in I$. 因此 $\ker\pi=I$. ■

命题 2.101 用一种非常简单的方式描述了$\mathbb{I}_m=\mathbb{Z}/(m)$中的同余类$[a]$. 这些同余类是用 m 去除后所有可能的余数的陪集：

$$\mathbb{I}_m=\{[0],[1],[2],\cdots,[m-1]\}.$$

一般情况下，R/I 的元素的描述不会如此简单. 另一方面，不久我们将看到(见定理 3.114)对 $k[x]/(f(x))$的元素的描述，其中 k 是域，$f(x)\in k[x]$. 293

注 因为读者十分熟悉群，所以定理 3.106 的证明可以被缩短一些. 若我们忽略交换环 R 中的乘法运算，则理想 I 是加法群 R 的子群. 因为 R 是阿贝尔群，所以子群 I 必定是正规的，因此商群 R/I 是可以定义的. 这样，交换环定义中的公理(i)到(iv)成立. 我们现在定义乘法，证明它是定义良好的，再验证公理(v)到(vii)成立. 命题 3.108 的证明也可以被缩短一些. 自然映射 $\pi: R\to R/I$ 是 R 的加法群到 R/I 的加法群的一个群同态，我们只需验证 $\pi(1)=1+I$ 以及 π 保持乘法运算即可.

→ **定理 3.109 (第一同构定理)** 若 $\varphi: R\to S$ 是一个交换环同态，则 $\ker\varphi$ 是 R 中的一个理想，$\mathrm{im}\varphi$ 是 S 的一个子环，且存在一个同构

$$\tilde{\varphi}: R/\ker\varphi \to \mathrm{im}\varphi,\quad a+\ker\varphi \mapsto \varphi(a).$$

证明 设 $I=\ker\varphi$. 在命题 3.38 中我们已看到：I 是 R 中的理想，$\mathrm{im}\varphi$ 是 S 的一个子环.

$\tilde{\varphi}$是定义良好的.

若 $a+I=b+I$，则 $a-b\in I=\ker\varphi$，因此 $\varphi(a-b)=0$. 但 $\varphi(a-b)=\varphi(a)-\varphi(b)$. 因此 $\tilde{\varphi}(a+I)=\varphi(a)=\varphi(b)=\tilde{\varphi}(b+I)$.

$\tilde{\varphi}$是一个同态.

首先，$\tilde{\varphi}(1+I)=\varphi(1)=1$.

其次，

$$\begin{aligned}\tilde{\varphi}((a+I)+(b+I)) &= \tilde{\varphi}(a+b+I)\\ &= \varphi(a+b)\\ &= \varphi(a)+\varphi(b)\\ &= \tilde{\varphi}(a+I)+\tilde{\varphi}(b+I).\end{aligned}$$

接着，

$$\begin{aligned}\tilde{\varphi}((a+I)(b+I)) &= \tilde{\varphi}(ab+I)\\ &= \varphi(ab)\\ &= \varphi(a)\varphi(b)\\ &= \tilde{\varphi}(a+I)\,\tilde{\varphi}(b+I).\end{aligned}$$

$\tilde{\varphi}$是满射. 若 $x\in\mathrm{im}\varphi$，则存在 $a\in R$ 使得 $x=\varphi(a)$，于是 $x=\tilde{\varphi}(a+I)$.

$\tilde{\varphi}$是单射. 若 $a+I\in\ker\tilde{\varphi}$，则$\tilde{\varphi}(a+I)=0$. 但$\tilde{\varphi}(a+I)=\varphi(a)$. 因此，$\varphi(a)=0$，$a\in$
294 $\ker\varphi=I$，$a+I=I=0+I$. 这样，$\ker\tilde{\varphi}=\{0+I\}$，$\tilde{\varphi}$是单射. ■

注 因为读者十分熟悉群，所以第一同构定理的证明可以被缩短一些. 若我们忽略乘法运算，则由定理 2.116 的证明可知由$\tilde{\varphi}(r+I)=\varphi(r)$给出的函数$\tilde{\varphi}: R/I\to\mathrm{im}\varphi$ 是加法群之间的一个群同构. 因为 $\varphi(1+I)=\varphi(1)=1$，所以我们只需证明$\tilde{\varphi}$保持乘法运算即可.

第一同构定理是说：若 $\varphi: R\to S$ 是一个同态，则在商环 $R/\ker\varphi$ 与子环 $\mathrm{im}\varphi$ 之间没有显著的差别，这是因为它们是同构的环. 第一基本定理还说明：一旦我们知道了同态的核和象，就可以从同态中建立一个同构. 因此，给定一个同态，我们应当首先描述它的核和象.（与群类似，环也有第二和第三同构定理，但它们比群的那些定理的作用要小. 与群类似，环也有对应定理. 我们现在不需要它，但我们会在命题 7.1 中加以证明.）

回忆一下，域 k 的素域是 k 的所有子域的交.

→ **命题 3.110** 若 k 是域，则它的素域同构于$\mathbb{Q}$ 或$\mathbb{F}_p$，其中 p 为某个素数.

证明 考虑同态 $\chi: \mathbb{Z}\to k$，$\chi(n)=n\cdot 1$，其中 1 是 k 中的单位元. 由于$\mathbb{Z}$ 中的每个理想都是主理想，所以存在整数 $m\geqslant 0$ 使得 $\ker\chi=(m)$. 若 $m=0$，则 χ 是单射，所以 $\mathrm{im}\chi$ 是 k 的一个子环，且同构于$\mathbb{Z}$. 由习题 3.51 知$\mathbb{Q}=\mathrm{Frac}(\mathbb{Z})\cong\mathrm{Frac}(\mathrm{im}\chi)$. 因为$\mathbb{Q}$ 是含$\mathbb{Z}$ 的最小域，所

以由习题 3.26 知 k 的素域同构于$\mathbb{Q}$．若 $m\neq0$，则由第一同构定理得$\mathbb{F}_m=\mathbb{Z}/(m)\cong\mathrm{im}\chi\subseteq k$．由于 k 是域，所以 $\mathrm{im}\chi$ 是整环，又由命题 3.12 知 m 是素数．若记 m 为 p，则 $\mathrm{im}\chi=\{0,1,2\cdot1,\cdots,(p-1)\cdot1\}$是 k 的子域且同构于$\mathbb{F}_p$．这样，由习题 3.26 知 $\mathrm{im}\chi\cong\mathbb{F}_p$ 是 k 的素域． ■

上述最后一个结果是将不同类型的域分类的第一步．

→ **定义** 若域 k 的素域同构于$\mathbb{Q}$，则称 k 有**特征 0**；若域 k 的素域同构于$\mathbb{F}_p$，p 为素数，则称 k 有**特征 p**.

域$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$，$\mathbb{C}(x)$的特征都为 0，后面三个域的任意子域的特征也为 0．每个有限域以某个素数 p 为特征，例如，$\mathbb{F}_p$ 上所有有理函数构成的函数域$\mathbb{F}_p(x)$的特征为素数 p.

回忆一下，若 R 是交换环，$r\in R$，$n\in\mathbb{N}$，则 $nr=r+\cdots+r$，这里有 n 个被加数．若 1 是 R 中的单位元，则 $nr=(n1)r$．这样，若 $n1=0$，则对所有 $r\in R$ 有 $nr=0$．现在，在$\mathbb{F}_p$ 中，我们有 $p[1]=[p]=[0]$，于是对所有$[r]\in\mathbb{F}_p$ 有 $p[r]=[0]$．更一般的，若 k 是以 $p>0$ 为特征的任意域，则对所有 $a\in k$ 有 $pa=0$．特别地，当 $p=2$ 时，我们有 $0=2a=a+a$，于是对所有 $a\in k$ 有 $-a=a$. 295

例 3.111 考虑赋值同态 $\varphi:\mathbb{R}[x]\to\mathbb{C}$，$f(x)\mapsto f(i)$，其中 $i^2=-1$，即 $\varphi:\sum_k a_kx^k\mapsto\sum_k a_ki^k$．第一同构定理告诉我们怎样求 $\mathrm{im}\varphi$ 和 $\ker\varphi$.

首先，φ 是满射：若 $a+bi\in\mathbb{C}$，则 $a+bi=\varphi(a+bx)\in\mathrm{im}\varphi$.

其次，

$$\ker\varphi=\{f(x)\in\mathbb{R}[x]:f(i)=0\},$$

即所有以 i 为根的多项式的集合．当然，$x^2+1\in\ker\varphi$，我们断言 $\ker\varphi=(x^2+1)$．因为$\mathbb{R}[x]$是一个 PID，所以理想 $\ker\varphi$ 是由次数最小的首一多项式生成的．假设 x^2+1 不能生成 $\ker\varphi$，则在$\mathbb{R}[x]$中存在 x^2+1 的线性因子，即 x^2+1 有实数根，矛盾．由第一同构定理得$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$.

因此，商环的构造从实数中建立了复数，即，即使我们不知道复数域，我们也可以用$\mathbb{R}[x]/(x^2+1)$定义它．用这种方法构造$\mathbb{C}$的一个优点是不必检验所有的域公理，$R[x]/(x^2+1)$自动是一个交换环，我们只需证明每个非零元素是单位． ◀

→ **命题 3.112** 若 k 是域，$I=(p(x))$，其中 $p(x)\in k[x]$是非常数多项式，则下列命题等价：

(i) $k[x]/I$ 是域.

(ii) $k[x]/I$ 是整环.

(iii) $p(x)$在 $k[x]$中不可约.

证明 (i)⇒(ii)．每个域都是整环.

(ii)⇒(iii)．假设 $p(x)$不是不可约的，则在 $k[x]$中存在一个分解 $p(x)=g(x)h(x)$满足 $\deg(g)<\deg(p)$，$\deg(h)<\deg(p)$．假设 $g(x)\in I=(p)$，则 $p(x)\mid g(x)$且 $\deg(p)\leqslant\deg(g)$，矛盾．这样，在 $k[x]/I$ 中 $g(x)+I\neq0+I$．类似地，在 $k[x]/I$ 中 $h(x)+I\neq0$．然而，乘积

$$(g(x)+I)(h(x)+I)=p(x)+I=0+I$$

在商环中是零元，这与 $k[x]/I$ 是整环矛盾．因此，$p(x)$是不可约多项式. 296

(iii)⇒(i). 设 $p(x)$ 是不可约的. 因为 $p(x)$ 不是单位, 所以理想 $I=(p(x))$ 不包含 1, 即, 在 $k[x]/I$ 中 $1+I\neq 0$. 若 $f(x)+I\in k[x]/I$ 不为零, 则 $f(x)\notin I$, 即 $f(x)$ 不是 $p(x)$ 的倍数, 换句话说, $p\nmid f$. 由引理 3.67, p 与 f 互素, 所以存在多项式 s 和 t 使得 $sf+tp=1$. 因此 $sf-1\in I$, 所以 $1+I=sf+I=(s+I)(f+I)$. 因此, $k[x]/I$ 的每个非零元都有逆元. 所以 $k[x]/I$ 是域. ■

比较该定理与命题 3.19, 则命题 3.19 可叙述为: $\mathbb{I}_m$ 是域, $\mathbb{I}_m$ 是整环与 m 是素数三者等价.

命题 3.113 (i)若 k 是域, $p(x)\in k[x]$ 是不可约多项式, 则 $k[x]/(p(x))$ 是一个域, 且包含 k(的同构物)和 $p(x)$ 的一个根 z.

(ii)若 $g(x)\in k[x]$, z 也是 $g(x)$ 的一个根, 则 $p(x)\mid g(x)$.

证明 (i)记 $(p(x))$ 为 I. 根据定理 3.112, 商环 $k[x]/I$ 是域, 这是因为 $p(x)$ 是不可约的. 由 $\varphi(a)=a+I$ 定义 $\varphi: k\to k[x]/I$, 因为 φ 是自然映射 $k[x]\to k[x]/I$ 对 k 的限制, 所以 φ 是一个同态. 由推论 3.45 知 φ 是一个单射(因为 k 是域), 于是 φ 是 k 到子域 $k^*=\{a+I: a\in k\}\subseteq k[x]/I$ 的一个同构.

记住 x 是 $k[x]$ 的一个特殊元素. 我们断言 $z=x+I\in k[x]/I$ 是 $p(x)$ 的一个根. 具体来讲, 令

$$p(x)=a_0+a_1x+\cdots+a_nx^n\in k[x],$$

其中对所有 i 有 $a_i\in k$. 我们不是把子域 $k^*\subseteq k[x]/I$ 和它的同构物 k 等同起来, 而是定义 $p^*(x)\in k^*[x]$ 如下:

$$p^*(x)=(a_0+I)+(a_1+I)x+\cdots+(a_n+I)x^n\in k^*[x],$$

我们证明 z 是 $p^*(x)$ 的一个根:

$$\begin{aligned}p^*(z)&=(a_0+I)+(a_1+I)z+\cdots+(a_n+I)z^n\\&=(a_0+I)+(a_1+I)(x+I)+\cdots+(a_n+I)(x+I)^n\\&=(a_0+I)+(a_1x+I)+\cdots+(a_nx^n+I)\\&=a_0+a_1x+\cdots+a_nx^n+I\\&=p(x)+I=I,\end{aligned}$$

因为 $p(x)\in I=(p(x))$. 但是 $I=0+I$ 是 $k[x]/I$ 的零元, 所以 z 是 $p^*(x)$ 的一个根.

(ii)因为 z 是 $g(x)$ 的一个根, 所以 $g(x)\in\ker\pi$, 其中 $\pi: k[x]\to k[x]/(p(x))$ 是自然映
297 射, 因此 $p(x)\mid g(x)$. ■

类似于推论 1.59 中把 $\mathbb{I}_m$ 描述为 $\{[0],[1],\cdots,[m-1]\}$, 下面这个定理也给出了 $k[x]/(f(x))$ 的一个更紧凑的描述. 虽然这个定理对任意多项式 $f(x)$ 都成立(不必不可约), 但 $f(x)$ 不可约是最重要的情形.

→ **定理 3.114** 设 k 是域, $f(x)\in k[x]$ 是 $n\geqslant 1$ 次非零多项式, 令 $I=(f(x))$. 则 $k[x]/(f(x))$ 中每个元素有如下的唯一表达式:

$$b_0+b_1z+\cdots+b_{n-1}z^{n-1},$$

其中 $z=x+I$ 是 $f(x)$ 的一个根, 且所有 $b_i\in k$.

证明 $k[x]/I$ 的每个元素有 $h(x)+I$ 的形式，其中 $h(x)\in k[x]$. 根据除法算式，存在多项式$q(x)$，$r(x)\in k[x]$使得 $h(x)=q(x)f(x)+r(x)$且 $r(x)=0$ 或 $\deg(r)<n=\deg(f)$. 由于 $h-r=qf\in I$，所以 $h(x)+I=r(x)+I$. 和命题 3.113 的证明一样，我们可以重写 $r(x)+I$ 为 $r(z)=b_0+b_1z+\cdots+b_{n-1}z^{n-1}$，所有 $b_i\in k$.

为证明唯一性，假设

$$r(z)=b_0+b_1z+\cdots+b_{n-1}z^{n-1}=c_0+c_1z+\cdots+c_{n-1}z^{n-1},$$

其中所有 $c_i\in k$. 定义 $g(x)\in k[x]$ 为 $g(x)=\sum\limits_{i=0}^{n-1}(b_i-c_i)x^i$. 因为 z 是 $g(x)$的一个根，所以由命题 3.113(ii) 知 $f(x)\mid g(x)$. 若 $g(x)$不是零多项式，则 $\deg(g)\geqslant n=\deg(f)$，这与 $\deg(g)<n$矛盾. 因此 $g(x)=0$，并且对所以 i 有 $b_i=c_i$. ■

把这个定理应用于例 3.111，其中 $f(x)=x^2+1\in\mathbb{R}[x]$，$n=2$，且陪集 $x+I$[其中 $I=(x^2+1)$]记为 i，我们看到每个复数有形如 $a+b\mathrm{i}$ 的唯一表达式，其中 a，$b\in\mathbb{R}$，且 $\mathrm{i}^2+1=0$，即 $\mathrm{i}^2=-1$. 在$\mathbb{C}$中作乘法，最容易的方法是先把 i 看作是一个变量，然后加上条件 $\mathrm{i}^2=-1$. 例如，为计算$(a+b\mathrm{i})(c+d\mathrm{i})$，首先写 $ac+(ad+bc)\mathrm{i}+bd\mathrm{i}^2$，然后观察 $\mathrm{i}^2=-1$. 在商环$k[x]/(p(x))$中计算乘积$(b_0+b_1z+\cdots+b_{n-1}z^{n-1})(c_0+c_1z+\cdots+c_{n-1}z^{n-1})$的恰当方法是首先把因子看作是 z 的多项式，然后加上条件 $p(z)=0$. 这些都是因为自然映射 $\pi: f(x)\mapsto f(x)+I$ 是一个同态. 因为 $\pi: f(x)\mapsto f(z)$，所以 $\pi(f)\pi(g)$是乘积 $f(z)g(z)$. 另一方面，计算 $\pi(fg)$应首先计算乘积 $f(x)g(x)$接着令 $x=z$.

→ **推论 3.115** *若 $g(x)\in\mathbb{F}_p[x]$是次数为 n 的不可约多项式，则 $k=\mathbb{F}_p[x]/(g(x))$是一个仅有 p^n 个元素的有限域.*

证明 由定理 3.112 知 k 是一个域，又由定理 3.114 知 k 中仅有 p^n 个元素. ■ 298

我们还不能断言存在仅有 p^n 个元素的域，这是因为我们还不知道在$\mathbb{F}_p[x]$中是否存在次数为 n 的不可约多项式(见习题 3.104).

我们现在推广例 3.111.

→ **定义** *设 E 是域，k 是它的子域. 若 $z\in E$，则定义 $k(z)$是 E 的包含 k 和 z 的最小子域，即 $k(z)$是 E 的所有包含 k 和 z 的子域的交. 我们称 $k(z)$为从**伴随着** z 的 k 中获得的域.*

例如，复数集$\mathbb{C}=\mathbb{R}(\mathrm{i})$是从伴随着 i 的$\mathbb{R}$中获得的.

→ **命题 3.116** *设 k 是域 K 的一个子域，且 $z\in K$.*

(i)若 z 是某个非零多项式 $f(x)\in k[x]$的根，则 z 是不可约多项式 $p(x)\in k[x]$的一个根，且 $p(x)\mid f(x)$.

(ii)若 $p(x)\in k[x]$是具有根 $z\in K$ 的不可约多项式，则存在一个同构

$$\varphi: k[x]/(p(x))\to k(z)$$

满足 $\varphi(x+(p(x)))=z$ 和对所有$a\in k$有 $\varphi(a)=a$.

(iii)若 z，$z'\in K$ 是 $p(x)$的两个根，则存在同构 $\theta: k(z)\to k(z')$满足 $\theta(z)=z'$和对所有 $a\in k$有 $\theta(a)=a$.

(iv)$k(z)$中每个元素有如下唯一表达式:

$$b_0+b_1z+\cdots+b_{n-1}z^{n-1},$$

其中 $b_i\in k$，$n=\deg(p)$.

证明 (i)由定理 3.84 知，存在一个分解：

$$f(x)=ap_1(x)\cdots p_m(x),$$

其中 $a\in k$ 是非零常数，$p_1(x)$，…，$p_m(x)$是 $k[x]$中首一不可约多项式．因为赋值 z 是一个环同态 $k[x]\to K$，所以

$$0=f(z)=ap_1(z)\cdots p_m(z).$$

299 但 K 是一个域，因而是一个整环．所以存在某个 i 使得 $p_i(z)=0$，即 z 是 $p_i(x)$的根.

(ii)由于 $p(x)$是不可约的，命题 3.112 表明 $k[x]/(p(x))$是一个域，因而 $\mathrm{im}\varphi$ 是一个域，即 $\mathrm{im}\varphi$ 是 K 的包含 k 和 z 的一个子域，所以 $k(z)\subseteq\mathrm{im}\varphi$．另一方面，$\mathrm{im}\varphi$ 中每个元素有形式 $g(x)+I$，其中 $g(x)\in k[x]$，所以 K 的包含 k 和 z 的任意子域 S 一定也包含 $\mathrm{im}\varphi$．因此 $\mathrm{im}\varphi=k(z)$.

(iii)和(ii)一样，存在同构 $\psi: k[x]/(p(x))\to k(z')$满足对所有 $a\in k$ 有 $\psi(a)=a$ 和 $\psi(x+(p(x)))=z'$．合成 $\theta=\psi\circ\varphi^{-1}$正是我们所要的同构.

(iv)令 $I=(p(x))$，由定理 3.114 知，$k[x]/I$ 中每个元素有如下唯一表达式 $b_0+b_1(x+I)+\cdots+b_{n-1}(x+I)^{n-1}$．同构 $k[x]/I\to k(z)$使得 $x+I\mapsto z$，该同构的单射性保证了表达式的唯一性. ■

推论 3.117 *设 k 是域，$p(x)\in k[x]$是不可约的，$\alpha\in k[x]/(p)$．若 α 是 $k[x]$中某个非零多项式的根，则存在以 α 作为根的唯一的首一不可约多项式 $h(x)\in k[x]$.*

注 *由命题 4.32 知关于 α 的假设是多余的.*

证明 命题 3.116(i)给出了一个以 α 作为根的不可约多项式 $h(x)\in k[x]$．显然，我们可以假定 $h(x)$是首一的.

为了证明 $h(x)$的唯一性，我们假设 $g(x)\in k[x]$也是以 α 作为根的首一不可约多项式．在 $k[x]/(p)$上有 $\gcd(h,g)\neq1$(因为 $x-\alpha$ 是公因子)，于是由推论 3.75 知在 $k[x]$中$(h,g)\neq1$．因为 $h(x)$是不可约的，所以它的首一因子只有 1 和它本身，所以$(h,g)=h$．因此，$h(x)\mid g(x)$．但因为 $g(x)$是首一不可约的，所以我们有 $h(x)=g(x)$. ■

我们现在证明两个重要结论：第一个结论是克罗内克(Kronecker)得到的，是说若 $f(x)\in k[x]$，其中 k 是任意一个域，则存在包含 k 和 $f(x)$的所有根的更大域 E；第二个是伽罗瓦得到的，他构造了不同于$\mathbb{F}_p$ 的有限域.

→ **定义** *多项式 $f(x)\in k[x]$在一个更大的域 K 上**分裂**，是指 $f(x)$是 $K[x]$中一些线性多项式的乘积.*

→ **定理 3.118 (克罗内克)** *若 k 是域，且 $f(x)\in k[x]$是非常数的，则存在一个包含 k 的域 K，使得 $f(x)$在 K 上分裂.*

证明 对 $\deg(f)$应用归纳法证明该定理．我们修改一下命题使得归纳步骤的证明更简单些：若 E 是包含 k 的一个域(这样 $f(x)\in k[x]\subseteq E[x]$)，则存在包含 E 的一个域 K 使得 $f(x)$是 $K[x]$中一些线性多项式的乘积．若 $\deg(f)=1$，则 $f(x)$是线性的，且我们可以选取 $K=E$.

对于归纳步骤，我们考虑两种情形．若 $f(x)$不是不可约的，则在 $k[x]$中 $f(x)=g(x)h(x)$，其中 $\deg(g)<\deg(f)$且 $\deg(h)<\deg(f)$．根据归纳假设，存在一个包含 k 的域 E 使得 $g(x)$在 E 上分裂；归纳假设还告诉我们，存在包含 E 的域 K 使得 $h(x)$在 K 上分裂．这样，$f(x)=$ 300
$g(x)h(x)$在 K 上分裂．第二种情形，在 $k[x]$中 $p(x)$是不可约的，则由命题 3.113(i)知存在一个包含 k 和 $p(x)$的根 z 的域 E．这样，在 $E[x]$中存在一个分解 $p(x)=(x-z)\ell(x)$．根据归纳假设，存在包含 E 的域 K 使得 $\ell(x)$在 K 上分裂，从而 $f(x)=(x-z)\ell(x)$在 K 上分裂．■

对于熟悉的域$\mathbb{Q}$，$\mathbb{R}$ 和$\mathbb{C}$，克罗内克定理没有给出任何新的东西．代数基本定理首先由高斯在 1799 年证明(完善了早期欧拉和拉格朗日的努力)，该定理是说每个非常数多项式 $f(x)\in\mathbb{C}[x]$在$\mathbb{C}$中有根．于是，根据对 $f(x)$的次数的归纳，$f(x)$的所有根都在$\mathbb{C}$中，即 $f(x)$在$\mathbb{C}$上分裂．另一方面，若 $k=\mathbb{F}_p$ 或 $k=\mathbb{C}(x)=\mathrm{Frac}(\mathbb{C}[x])$，则应用克罗内克定理我们知道，对任意给定的 $f(x)$，总是存在某个更大的域 E 包含 $f(x)$的所有根．例如，存在包含$\mathbb{C}(x)$和$\sqrt{x}$的域．代数基本定理有一个更一般的叙述：每个域 k 是一个**代数闭域** K 的子域，即，K 是包含 k 的域且使得每个 $f(x)\in k[x]$是 $K[x]$中的一些线性多项式的乘积．相反地，克罗内克定理一次只给出一个多项式的根．

我们现在考查有限域，即只有有限个元素的域．我们首先证明有限域中元素的个数是素数的幂．我们给出习题 3.105 的群论证法．

→ **定义**　*在有限域 E 中，若每个非零元素 $a\in E$ 都等于 $\pi\in E$ 的某个幂，则称 π 是 E 的***本原元素**．

→ **命题 3.119**　(i)*若 E 是有限域，则 E 有本原元素．*

(ii)*若 E 是特征为 p 的有限域且其素域为 k，则存在 $n\geq 1$ 使得 $|E|=p^n$．*

证明　(i)因为 E 是有限的，所以它的乘法群 $E^\times$ 是循环群．由定理 3.55 知 $E^\times$ 的生成元就是 E 的本原元素．

(ii)因为 E 的每个元素都等于 π 的某个幂，所以 $E=k(\pi)$．由 E 的有限性知序列 1，π，π^2，π^3，…存在一个重复，即存在正整数 $r>s$ 满足 $\pi^r=\pi^s$．因此 $\pi^{r-s}=1$，这样 π 是 $x^{r-s}-1$ 的根．根据定理 3.116(i)，存在不可约多项式 $g(x)\in k[x]$以 π 作为根，又由定理 3.116(ii)知存在一个同构 $k[x]/(g(x))\cong k(\pi)=E$．若 $\deg(g)=n$，则由推论 3.115 知 $|E|=p^n$．■

我们现在将展示有限域．

→ **定理 3.120 (伽罗瓦)**　*若 p 是素数，n 是正整数，则存在恰有 p^n 个元素的域．* 301

证明　记 $q=p^n$，并考虑多项式

$$g(x)=x^q-x\in\mathbb{F}_p[x].$$

根据克罗内克定理，存在包含$\mathbb{F}_p$ 的域 E 使得 $g(x)$是 $E[x]$中一些线性因子的乘积．定义

$$F=\{\alpha\in E: g(\alpha)=0\},$$

则 F 是由 $g(x)$的所有根构成的集合．因为导数 $g'(x)=qx^{q-1}-1=p^nx^{q-1}-1=-1$，所以 $\gcd(g,g')=1$．根据习题 3.67，$g(x)$的所有根是互异的，即 F 恰有 $q=p^n$ 个元素．

我们断言 F 是 E 的子域，由此可以完成这个证明．若 a，$b\in F$，则 $a^q=a$，$b^q=b$．因此，$(ab)^q=a^qb^q=ab$，这样 $ab\in F$．根据习题 3.97，$(a-b)^q=a^q-b^q=a-b$，所以 $a-b\in F$．最

后，若 $a\neq 0$，则对 $a^q=a$ 应用消去律得 $a^{q-1}=1$，所以 a 的逆元是 a^{q-2}(位于 F 中，因为 F 在乘法下是封闭的)． ■

在推论 5.25 中，我们将在看到元素个数相同的两个有限域是同构的.

例 3.121 在习题 3.19 中，我们构造了一个含 4 个元素的域 k，其元素是矩阵 $\begin{bmatrix} a & b \\ a & a+b \end{bmatrix} = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$，其中 $a,b\in\mathbb{I}_2$. $\left(\text{我们可以看到}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\text{是本原元素，}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\text{也是.}\right)$

另一方面，我们还可以构造一个含 4 个元素的域，它是商环 $F=\mathbb{F}_2[x]/(x^2+x+1)$，其中 $x^2+x+1\in\mathbb{F}_2[x]$是不可约的. 根据推论 3.114，$F$ 是由所有形如 $a+bz$ 的元素构成的域，其中 z 是 x^2+x+1 的一个根，$a,b\in\mathbb{F}_2$. 由于 $z^2+z+1=0$，所以有 $z^2=-z-1=z+1$. 另外，$z^3=zz^2=z(z+1)=z^2+z=1$. 现在容易看出，存在一个环同构 $\varphi: k\to F$ 满足 $\varphi: \begin{bmatrix} a & b \\ a & a+b \end{bmatrix}\mapsto a+bz$. ◀

例 3.122 根据例 3.99 中的表可以知道，$\mathbb{F}_3[x]$中存在三个首一不可约二次多项式，即

$$p(x)=x^2+1,\quad q(x)=x^2+x-1,\text{和 } r(x)=x^2-x-1;$$

每个多项式产生一个含有 $9=3^2$ 个元素的域. 让我们详细地说说头两个. 根据推论 3.114，若 $E=\mathbb{F}_3[x]/(q(x))$，则

$$E=\{a+b\alpha: \text{其中 } \alpha^2+1=0\}.$$

类似地，若 $F=\mathbb{F}_3[x]/(p(x))$，则

302 $$F=\{a+b\beta: \text{其中 } \beta^2+\beta-1=0\}.$$

读者可以检验由

$$\varphi(a+b\alpha)=a+b(1-\beta)$$

定义的 $\varphi: E\to F$ 是一个同构，从而证明这两个域是同构的.

现在$\mathbb{F}_3[x]/(x^2-x-1)$也是一个含 9 个元素的域，且我们可以证明它与上述给出的两个域 E 和 F 都是同构的.

在例 3.99 中，我们已经展示了 8 个首一不可约三次多项式 $p(x)\in\mathbb{F}_3[x]$，它们中每一个都产生一个含有 $27=3^3$ 个元素的域$\mathbb{F}_3[x]/(p(x))$. 这 8 个域都是同构的. ◀

在第 4 章关于编码的那节中，我们将看到在从太空到地球传送数据的过程中有限域是一个基本因素.

习题

H 3.92 判断对错并说明理由.

(i)若 I 是交换环 R 的一个真理想，$\pi: R\to R/I$ 是自然映射，则 $\ker\pi=I$.

(ii)若 I 是交换环 R 的一个真理想，$\pi: R\to R/I$ 是自然映射，则 π 是满射.

(iii)若 $f: R\to S$ 是交换环的一个同态，则 S 有与 $R/(\ker f)$同构的子环.

(iv)若 I 是交换环 R 的一个真理想，则 R 有与 R/I 同构的子环.

(v)若 p 是一个素数，则特征为 p 的每个域是有限域.

(vi)特征为 0 的域都是无限域.

(vii)若 $f(x)$是域 k 上的不可约多项式，则 $k[x]/(f(x))$是一个域.

(viii)若 $f(x)$是域 k 上的非常数多项式，且商环 $k[x]/(f(x))$是一个域，则 $f(x)$是不可约的.

(ix)若 $f(x)$是域 k 上的不可约多项式，则每个元素 $z\in k[x]/(f(x))$是 $f(x)$的一个根.

(x)若 $k\subseteq K$ 都是域，且 $z\in K$ 是某个非零多项式 $p(x)\in k[x]$的根，则 $p(x)$在 $k[x]$中不可约.

(xi)存在一个域包含$\mathbb{C}(x)$和 $\sqrt{x+\mathrm{i}}$.

(xii)对每个正整数 n，存在一个域恰有 11^n 个元素.

(xiii)对每个正整数 n，存在一个域恰有 10^n 个元素.

(xiv)对每个正整数 n，存在一个域恰有 9^n 个元素.

(xv)存在特征为 2 的域 E，使得 x^4+x+1 是 $E[x]$中线性因子的积.

3.93 对每个交换环 R，证明 $R[x]/(x)\cong R$. 303

3.94 (**$k[x]$中的中国剩余定理**)

H (i)证明，若 k 是域，且 $f(x)$，$f'(x)\in k[x]$互素，则给定 $b(x)$，$b'(x)\in k[x]$，存在 $c(x)\in k[x]$满足

$$c-b\in(f)\text{ 和 }c-b'\in(f')；$$

而且，若 $d(x)$是另一个公共解，则 $c-d\in(ff')$.

H (ii)证明，若 k 是域，且 $f(x)$，$g(x)\in k[x]$互素，则

$$k[x]/(f(x)g(x))\cong k[x]/(f(x))\times k[x]/(g(x)).$$

***H** 3.95 证明，若 k 是特征为 0 的域，且 $p(x)\in k[x]$是一个不可约多项式，则 $p(x)$没有重根，从而推广了习题 3.84.

3.96 (i)证明域 K 不能有满足 $k'\cong\mathbb{Q}$ 和 $k''\cong\mathbb{F}_p$ 的子域 k' 和 k''，其中 p 为某个素数.

(ii)证明域 K 不能有满足 $k'\cong\mathbb{F}_p$ 和 $k''\cong\mathbb{F}_q$ 的子域 k' 和 k''，其中 $p\neq q$.

*3.97 设 p 是素数且 $q=p^n$，$n\geqslant1$.

H (i)证明函数 $F:\mathbb{F}_q\to\mathbb{F}_p$，$F(a)=a^p$，是一个同构(F 称为**弗洛贝尼乌斯(Frobenius)映射**).

(ii)证明每个元素 $a\in\mathbb{F}_q$ 有一个 p 次根，即存在 $b\in\mathbb{F}_q$ 满足 $a=b^p$.

(iii)设 k 是特征为 $p>0$ 的域. 对每个正整数 n，证明环同态 $F_n:k\to k$，$F_n(a)=a^{p^n}$，是单射.

***H** 3.98 证明有限域 E 中的每个元素 z 都是两个平方数的和. (若 $z=a^2$ 是一个平方数，则我们可以写为 $z=a^2+0^2$.)

***H** 3.99 若 p 是素数且 $p\equiv3 \bmod 4$，证明 $a^2\equiv2 \bmod p$ 或 $a^2\equiv-2 \bmod p$ 有解.

*3.100 (i)证明 x^4+1 在$\mathbb{F}_2[x]$中可分解.

H (ii)若 $x^4+1=(x^2+ax+b)(x^2+cx+d)\in\mathbb{F}_p[x]$，其中 p 是奇素数. 证明 $c=-a$ 和

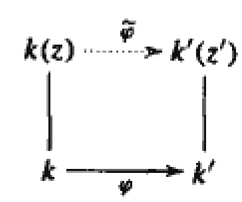
$$d+b-a^2=0$$
$$a(d-b)=0$$
$$bd=1.$$

H (iii)证明 x^4+1 在$\mathbb{F}_p[x]$中可分解当且仅当下述同余方程都有解，其中 p 是奇素数：

$$b^2\equiv-1 \bmod p,$$
$$a^2\equiv\pm2 \bmod p.$$

H (iv)证明，对所有素数 p，x^4+1 在$\mathbb{F}_p[x]$中可分解.

*3.101 推广命题 3.116(iii)如下. 设 $\varphi:k\to k'$是域之间的同构，E/k 和 E'/k'是扩张，$p(x)\in k[x]$和 $p^*(x)\in k'[x]$都是不可约多项式(和在定理 3.33 中一样，若 $p(x)=\sum a_ix^i$，则 $p^*(x)=\sum\varphi(a_i)x^i$)，并设 $z\in E$ 和 $z'\in E'$分别是 $p(x)$和 $p^*(x)$的根，则存在一个同构$\tilde{\varphi}$: $k(z)\to k'(z')$，满足$\tilde{\varphi}(z)=z'$以及$\tilde{\varphi}$扩张了 φ. 304



*3.102　设 $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n\in k[x]$，其中 k 是一个域，并假设 $f(x)=(x-r_1)(x-r_2)\cdots(x-r_n)\in E[x]$，其中 E 是包含 k 的域. 证明

$$a_{n-1}=-(r_1+r_2+\cdots+r_n)\text{ 和 }a_0=(-1)^n r_1r_2\cdots r_n.$$

由此得出 $f(x)$ 的所有根的和与积都在 k 中.

H 3.103　若 $E=\mathbb{F}_2[x]/(p(x))$，其中 $p(x)=x^3+x+1$，则 E 是含 8 个元素的域. 证明 $p(x)$ 的一个根 π 是 E 的一个本原元素，即把 E 的每个非零元素写成 π 的幂.

*3.104　(i)证明，对所有 $n\geq1$，$\mathbb{Q}[x]$中存在次数为 n 的不可约多项式.

H (ii)证明，对所有 $n\geq1$ 和每个素数 p，$\mathbb{F}_p[x]$中存在次数为 n 的不可约多项式.

(iii)证明，对所有 $n\geq1$ 和每个有限域 k，$k[x]$中存在次数为 n 的不可约多项式.

*H 3.105　若 E 是一个有限域，利用定理 2.147 即柯西定理证明，$|E|=p^n$ 对某个素数 p 和某个 $n\geq1$ 成立.

3.9　一个数学历程

3.9.1　拉丁方

1782 年，欧拉在他一篇关于魔方的文章中提出了下述问题. 假设有属于 6 种官衔的 36 个军官，他们来自 6 个不同的团. 若给这 6 个团标上 1 到 6 的号码，并设这 6 种官衔为上尉，少校，中尉，…，则每个军官有一个双重标签(例如上尉 3 或少校 4). 欧拉问，是否可将这些军官排成 6 行 6 列，使得每一行军官的军衔各不相同，所属的团也各不相同，且每一列也是如此. 因此任一行不能有属于同一个团的军官，任一列也是如此.

根据下述定义这个问题可以说得更清楚些.

定义　一个 $n\times n$ **拉丁方**是指一个 $n\times n$ 矩阵，其元素取自一个含 n 个元素的集合 X(例如

305 $X=\{0,1,\cdots,n-1\}$)，使得矩阵的任一行和任一列都没有出现两个相同的元素.

容易看出，一个 $n\times n$ 矩阵 A (其元素取自一个集合 X，$|X|=n$)是一个拉丁方，当且仅当 A 的每一行和每一列都是 X 的一个置换.

根据习惯，我们可把矩阵 A 记为 $A=[a_{ij}]$，其中 a_{ij} 是其元素，第一个指标 i 描述第 i 行

$$a_{i1}a_{i2}\cdots a_{in},$$

第二个指标 j 描述第 j 列

$$\begin{matrix}a_{1j}\\a_{2j}\\\vdots\\a_{nj}\end{matrix}$$

例 3.123　元素为 0 和 1 的 2×2 拉丁方恰有 2 个：

$$A=\begin{bmatrix}0&1\\1&0\end{bmatrix}\quad\text{和}\quad B=\begin{bmatrix}1&0\\0&1\end{bmatrix}$$ ◀

例 3.124 以下是 2 个 4×4 拉丁方.

$$A=\begin{bmatrix}0&1&2&3\\1&0&3&2\\2&3&0&1\\3&2&1&0\end{bmatrix}\quad 和 \quad B=\begin{bmatrix}0&1&2&3\\2&3&0&1\\3&2&1&0\\1&0&3&2\end{bmatrix}$$ ◀

例 3.125 阶为 n 的有限群 $G=\{a_1, \cdots, a_n\}$ 的乘法表，即 $[a_ia_j]$，是一个拉丁方. 因为群中消去律成立，所以由 $a_ia_j=a_ia_k$ 可推出 $a_j=a_k$，所以第 i 行是 G 的一个置换；因为由 $a_ia_\ell=a_ja_\ell$ 可推出 $a_i=a_j$，所以第 j 列是 G 的一个置换. ◀

我们将利用下面的构造，它通常是一个新手定义矩阵乘法的第一种尝试.

定义 若 $A=[a_{ij}]$ 和 $B=[b_{ij}]$ 都是 $m\times n$ 矩阵，则它们的**阿达马积(Hadamard product)**，记为 $A\circ B$ 是指一个 $m\times n$ 矩阵，其 ij 元素是有序对 (a_{ij}, b_{ij}).

若 A 和 B 的元素位于一个交换环 R 中，则我们通常用 R 中的积 $a_{ij}b_{ij}$ 代替阿达马积的 ij 元素 (a_{ij}, b_{ij}).

假设 A 的元素位于满足 $|X|=n$ 的集合 X 中，且 B 的元素位于满足 $|Y|=n$ 的集合 Y 中. $X\times Y$ 中恰有 n^2 个有序对，且我们说 A 和 B 是正交的，若每个有序对是阿达马积 $A\circ B$ 中的一个元素. 306

定义 两个 $n\times n$ 拉丁方 $A=[a_{ij}]$ 和 $B=[b_{ij}]$，它们的元素分别位于集合 X 和 Y 中且 $|X|=n=|Y|$，它们称为是**正交的**，若它们的阿达马积 $A\circ B$ 中的所有元素即所有有序对 (a_{ij}, b_{ij}) 都是互异的.

不存在一对正交的 2×2 拉丁方：正如我们在例 3.123 中所看到的，元素在 $X=\{0, 1\}$ 中的 2×2 拉丁方只有 2 个，且它们的阿达马积是

$$A\circ B=\begin{bmatrix}01&10\\10&01\end{bmatrix}.$$

只有两个不同的有序对，而定义要求的是四个.

例 3.126 例 3.124 中的两个 4×4 拉丁方是正交的，因为 16 个有序对是互不相同的.

$$A\circ B=\begin{bmatrix}00&11&22&33\\12&03&30&21\\23&32&01&10\\31&20&13&02\end{bmatrix}$$ ◀

设 A 是一个矩阵，其元素位于集合 X 中. 若 $\alpha: x\mapsto x'$ 是 X 的一个置换，则对 A 中的每个元素应用 α 就能得到新的矩阵 A'. 详细地说，若 $x=a_{ij}$ 是 A 的 ij 元素，则 x' 是 A' 的 ij 元素，所以 $A'=[(a_{ij})']$.

引理 3.127 设 $A=[a_{ij}]$ 是一个拉丁方，其元素位于含 n 个元素的集合 X 中. 若 $x\mapsto x'$ 是 X 的一个置换，则 $A'=[(a_{ij})']$ 是一个拉丁方. 而且，若 A 和 $B=[b_{ij}]$ 是正交的拉丁方，则 A' 和 B 也是正交的.

证明 因为 A 的第 i 行(a_{i1}, …, a_{in})是 X 的一个置换，所以 A' 的第 i 行($(a_{i1})'$, …, $(a_{in})'$)也是 X 的一个置换(两个置换的合成还是一个置换). 类似的讨论表明，A' 的列是 X 的置换，所以 A' 是一个拉丁方.

若 A' 和 B 不正交，则 $A'\circ B$ 有两个元素相等，不妨设(a'_{ij}, b_{ij})=($a'_{k\ell}$, $b_{k\ell}$)，所以 $a'_{ij}=a'_{k\ell}$, $b_{ij}=b_{k\ell}$，所以 $a_{ij}=a_{k\ell}$. 因此，$A\circ B$ 中存在一个重复的有序对，这与 A 和 B 正交相矛盾，因而 A' 和 B 是正交的. ■

欧拉问题是问，是否存在一对正交的 6×6 拉丁方(第一个指标表示官衔，第二个指标表示
307 团号). 为了弄明白他为什么关心 $n=6$ 的情形，让我们先构造一些正交对.

命题 3.128 (i)若 k 是一个有限域，$a\in k^{\times}=k-\{0\}$，则 $|k|\times|k|$ 矩阵
$$L_a=[\ell_{xy}]=[ax+y],$$
是一个拉丁方，其中 x, $y\in k$.

(ii)若 a, $b\in k^{\times}$ 且 $a\neq b$，则 L_a 和 L_b 是正交的拉丁方.

证明 (i)L_a 的第 x 行由元素 $ax+y$ 构成，其中 x 是固定的. 这些元素是互异的，因为若 $ax+y=ax+y'$，则 $y=y'$. 类似地，L_a 的第 y 列由元素 $ax+y$ 构成，其中 y 是固定的，且这些元素互异，因为由 $ax+y=ax'+y$ 可推出 $ax=ax'$. 因为 $a\neq 0$，所以由消去律得 $x=x'$.

(ii)假设有两个有序对相等，不妨设为
$$(ax+y,bx+y)=(ax'+y',bx'+y').$$
则 $ax+y=ax'+y'$, $bx+y=bx'+y'$. 所以有
$$a(x-x')=y'-y=b(x-x').$$
因为 $a\neq b$，由消去律得 $x-x'=0$，因而 $y'-y=0$，即 $x'=x$, $y'=y$. 因此，L_a 和 L_b 是正交的拉丁方. ■

推论 3.129 对每个素数幂 $p^e>2$，存在一对正交的 $p^e\times p^e$ 拉丁方.

证明 根据伽罗瓦定理，存在一个有限域 k 满足 $|k|=p^e$. 为了有一对正交的拉丁方，我们需要 $|k^{\times}|\geqslant 2$，即 $p^e-1\geqslant 2$，因而 $p^e>2$. ■

注 大约在1830年伽罗瓦才发明了有限域，欧拉在1782年用另一种(更复杂的)方法构造了正交的 $p^e\times p^e$ 拉丁方.

我们现在展示如何从小的正交拉丁方中创建大的正交拉丁方. 设 K 和 L 都是集合，满足 $|K|=k$, $|L|=\ell$. 若 $B=[b_{ij}]$ 是元素取自 L 的 $\ell\times\ell$ 矩阵，则 aB 是 $\ell\times\ell$ 矩阵，其 ij 元素是 ab_{ij}[其中 ab_{ij} 是有序对(a, b_{ij})的缩写]. 若 $A=[a_{st}]$ 是一个 $k\times k$ 矩阵，其元素取自 K，则 A 和 B 的克罗内克积 $A\otimes B$ 是一个 $k\ell\times k\ell$ 矩阵

308
$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1k}B \\ a_{21}B & a_{22}B & \cdots & a_{2k}B \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1}B & a_{k2}B & \cdots & a_{kk}B \end{bmatrix}.$$

定理 3.130（欧拉） 若 $n \not\equiv 2 \bmod 4$，则存在一对正交的 $n \times n$ 拉丁方.

证明 我们只陈述证明的主要步骤. 首先证明，若 A 和 B 都是拉丁方，则 $A \otimes B$ 也是拉丁方. 其次证明，若 A 和 A' 是正交的 $k \times k$ 拉丁方，且 B 和 B' 是正交的 $\ell \times \ell$ 拉丁方，则 $A \otimes B$ 和 $A' \otimes B'$ 都是正交的 $k\ell \times k\ell$ 拉丁方. 这几步都不会很难. 当然，我们可以构造有限多个矩阵的克罗内克积.

若 n 是一个正整数，我们断言 $n \equiv 2 \bmod 4$ 当且仅当存在一个奇数 m 满足 $n=2m$. 若 $n \equiv 2 \bmod 4$，则 $n-2=4k$，k 为某个整数，且 $n=2(2k+1)$. 反之，若 $n=2m$，m 是奇数，则 $n=2m=2(2d+1)=4d+2$，所以 $n-2=4d$. 于是 $n \not\equiv 2 \bmod 4$ 当且仅当 $n=2^e p_1^{e_1} \cdots p_t^{e_t}$，其中 $e \neq 1$，且 p_i 都是奇素数. 根据推论 3.129，对每个 i，存在一对正交的 $p_i^{e_i} \times p_i^{e_i}$ 拉丁方，且若 $e \geqslant 2$，则还有一对正交的 $2^e \times 2^e$ 拉丁方. 取这些拉丁方的克罗内克积，则得一对正交的 $n \times n$ 拉丁方. ■

使欧拉定理不成立的最小的 n 是 6，这就是欧拉提出 36 个军官问题的原因. 事实上，他猜想若 $n \equiv 2 \bmod 4$，则不存在正交的 $n \times n$ 拉丁方. 1901 年，泰利(G. Tarry)证明不存在正交的 6×6 拉丁方，因而回答了这一节的欧拉问题：不存在符合要求的 36 个军官的排列. 但是，1958 年，帕克(E. T. Parker)发现了一对正交的 10×10 拉丁方，从而证明欧拉猜想是不对的. 表 3-1 就是帕克举出的例子，我们注意到每个小于 100 的数都以十进制数字作为一个元素出现. 帕克，博泽(R. C. Bose)和施理克汉德(S. S. Shrikhande)继续证明了，除了 $n=2$ 和 6 之外，对其他所有的 n 都存在一对正交的 $n \times n$ 拉丁方.

表 3-1

00	15	23	32	46	51	64	79	87	98
94	77	10	25	52	49	01	83	68	36
71	34	88	17	20	02	43	65	96	59
45	81	54	66	18	27	72	90	39	03
82	40	61	04	99	16	28	37	53	75
26	62	47	91	74	33	19	58	05	80
13	29	92	48	31	84	55	06	70	67
69	93	35	50	07	78	86	44	12	21
57	08	76	89	63	95	30	11	24	42
38	56	09	73	85	60	97	22	41	14

309

3.9.2 幻方

我们现在利用正交拉丁方构造一些幻方.

定义 一个 $n \times n$ **幻方**是指一个 $n \times n$ 矩阵 $A=[a_{ij}]$，其元素由 $0, 1, \cdots, n^2-1$ 构成，且行和与列和都相等，即存在一个数 σ，称为**幻数**，满足

$$\text{对所有 } i, \sum_{j=1}^{n} a_{ij} = \sigma; \quad \text{对所有 } j, \sum_{i=1}^{n} a_{ij} = \sigma.$$

图 3-2 是德国名画家阿尔布雷特·丢勒(Albrecht Dürer)在 1514 年雕刻的版画《忧郁症》(Melencolia I)，它的右上角就是右侧的方格.

注意创作年代 1514 位于最下面一行[⊖]. 行和与列和都等于 34. 实际上，对角线上所有项的和 $\sum_i a_{ii}$ 也是 34，**反对角线**（从左下角到右上角的连线）上所有项的和也是 34. 这不是一个幻方，因为它的元素是从 1 变到 16，而不是从 1 变到 15，但是这很容易补救：将每个元素减去 1 就得一个幻方，其幻数为 30.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1



图 3-2

命题 3.131 *若 A 是一个 $n\times n$ 幻方，则其幻数为*

$$\sigma=\frac{1}{2}n(n^2-1).$$

证明 若 ρ_i 表示 A 的第 i 行中元素的总和，则对所有 i 有 $\rho_i=\sigma$，所以 $\sum_{i=1}^{n}\rho_i=n\sigma$. 但是，$n\sigma$ 是 A 中所有元素的总和，即

$$n\sigma=1+2+\cdots+(n^2-1)=\frac{1}{2}(n^2-1)n^2.$$

因此 $\sigma=\frac{1}{2}n(n^2-1)$. ■

若 $n=4$，则 $\sigma=\frac{1}{2}\cdot 4\cdot 15=30$.

⊖ 丢勒很熟悉犹太教的神秘学，它里面的字母表中每个字母对应一个数，且每个单词对应其字母的值的总和. 拉丁字母表的字母对应的数是 1，2，…，26. 注意到，在这个幻方中 4 和 1 位于 1514 的两侧，这两个数对应艺术家阿尔布雷特·丢勒(Dürer, Albrecht)的首写字母.

关于术语有一点小小的不同看法. 为了使一个方格成为一个幻方，一些作者也要求对角线上元素的和与反对角线上元素的和都等于幻数，正如在修改后的丢勒方格中那样. [310~311]

定义 *一个**魔方**是指一个幻方，其对角线和反对角线上的元素之和都等于幻数.*

下面将会构造一些魔方，不过我们先回到对幻方的讨论中. 构造幻方有很多方法. 例如，在 1693 年，笛拉卢培(De la Loubère)展示了怎样构造一个 $n\times n$ 幻方，n 是任意奇数，其中 0 可以出现在任意 ij 位置(看史达克(Stark)的《数论导引》(An Introduction to Number Theory)第四章). 我们现在利用正交拉丁方构造幻方.

命题 3.132 *若 $A=[a_{ij}]$和 $B=[b_{ij}]$都是元素为 0，1，…，$n-1$ 的正交拉丁方，则矩阵 $M=[a_{ij}n+b_{ij}]$是一个 $n\times n$ 幻方.*

证明 因为 A 和 B 正交，所以它们的阿达马积 $A\circ B$ 的所有元素(a_{ij}, b_{ij})是互不相同的. 由命题 1.47，即一个非负数的 n-进位数字是唯一的，可知 0 到 n^2-1 的每个数都出现在 M 中(注意到，$0\leqslant a_{ij}<n$ 和 $0\leqslant b_{ij}<n$). A 是一个拉丁方是指 A 的每行和每列都是 0，1，…，$n-1$ 的一个置换，所以每行和每列的总和都等于 $s=\sum_{i=0}^{n-1}i=\frac{1}{2}(n-1)n$. 类似地，$B$ 的每行和每列的总和也等于 s. 因此，M 的每行的总和等于 $sn+s$，其每列的总和也是 $sn+s$. 因此，M 是一个幻方. ■

M 的幻数是 $\sigma=s(n+1)$，其中 $s=\frac{1}{2}n(n-1)$，这与命题 3.131 中幻数的值相同，这是因为 $s(n+1)=\frac{1}{2}n(n-1)(n+1)=\frac{1}{2}n(n^2-1)$.

帕克的 10×10 正交拉丁方已经被转变成表 3-1 所示的十进制数字，它是刚才所构造的幻方的一个例子.

例 3.133 命题 3.132 不是构造幻方的唯一方法. 例如，这里有一个 6×6 幻方(当然其幻数是 105)，它还是一个魔方. 这个幻方不是从一对正交的 6×6 拉丁方产生的，因为泰利已经告诉我们，没有这样的 6×6 的拉丁方.

34	0	5	25	18	23
2	31	6	20	22	24
30	8	1	21	26	19
7	27	32	16	9	14
29	4	23	11	13	15
3	35	28	12	17	10

◀

我们现在从正交拉丁方中构造一些魔方. 已经知道，对所有 $n\geqslant 3$ 都有 $n\times n$ 魔方存在，但是我们将只对某些 n 构造魔方. [312]

定义 *元素位于集合 X 中 ($|X|=n$)的 $n\times n$ 拉丁方称为**对角拉丁方**，若其对角线和反对角线都是 X 的一个置换.*

引理 3.134 *若 n 是一个正奇数且不是 3 的倍数，则存在一对正交的 $n\times n$ 对角拉丁方.*

证明 我们先构造一个 $n\times n$ 对角拉丁方. 将行和列标号使得 $0\leqslant i$，$j\leqslant n-1$ 是很方便的. 定义 A 为一个 $n\times n$ 矩阵，其 ij 元素是模 n 的同余类$[i+2j]$. 我们省略元素的中括号从而简化记号. 因此

$$A=\begin{bmatrix} 0 & 2 & 4 & \cdots & 2(n-1) \\ 1 & 3 & 5 & \cdots & 1+2(n-1) \\ 2 & 4 & 6 & \cdots & 2+2(n-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n-1 & n+1 & n+3 & \cdots & 3(n-1) \end{bmatrix}.$$

现在证明 A 是一个对角拉丁方，记住它的元素位于$\mathbb{I}_n$ 中. 每行是一个置换：对固定的 i，若 $i+2j=i+2j'$，则 $2(j-j')\equiv 0 \bmod n$. 但是，因为 n 是奇数，所以$(2, n)=1$，所以$[j]=[j']$. 每列是一个置换：对固定的 j，若 $i+2j=i'+2j$，则 $i-i'\equiv 0 \bmod n$，即$[i]=[i']$. 对主对角线，若 $i+2i=i'+2i'$，则 $3i=3i'$. 因为 $3\nmid n$，所以有$[i]=[i']$. 最后，对反对角线，若 $i+2(n-i)=i'+2(n-i')$，则$-i=-i'$，所以$[i]=[i']$.

显然，A 的转置 A^{T} 也是一个对角拉丁方，我们现在证明 A 和 A^{T} 是正交的[⊖]. 注意到，A^{T} 的ij元素是 $j+2i$，所以阿达马积 $A\circ A^{\mathrm{T}}$ 的 ij 元素是$(i+2j, j+2i)$. 为验证正交性，假设$(i+2j, j+2i)=(i'+2j', j'+2i')$. 因为 $i+2j=i'+2j'$ 和 $j+2i=j'+2i'$（记住元素位于$\mathbb{I}_n$ 中)，所以$[i-i']=[j-j']$和$[2(j'-j)]=[i-i']$. 用$[2]$乘第二个等式得$[4(j'-j)]=[2(i-i')]=[j'-j]$. 现在$[4(j'-j)]=[j'-j]$，因而 $3(j'-j)\equiv 0 \bmod n$. 但是 $3\nmid n$，所以 $j'-j\equiv 0 \bmod n$，$[j]=[j']$. 类似的讨论可得$[i]=[i']$. ■

命题 3.135 *若 n 是一个正奇数且不是 3 的倍数，则存在一个 $n\times n$ 魔方.*

证明 由引理 3.134 知，存在 $A=[a_{ij}]$，$B=[b_{ij}]$都是正交的 $n\times n$ 对角拉丁方. 根据

313 命题 3.132，矩阵 $M=[a_{ij}n+b_{ij}]$是一个幻方，其幻数是 $\sigma=s(n+1)$，其中 $s=\sum_{i=0}^{n-1} i$. 因为 A 的主对角线和 B 的主对角线都是$\{0, 1, \cdots, n-1\}$的置换，所以对角线上所有元素的和是 $s(n+1)$，反对角线上所有元素的和也是 $s(n+1)$. ■

3.9.3 试验设计

以下是关于肥料的问题，我们最终可以看出它与拉丁方有联系. 为使谷类产量最大化，农夫不得不选择最佳的播种方法. 但他知道肥料的用量也会影响产量. 他怎样才能设计一个试验使得这两个的组合是最佳的呢？我们给出一个简单的说明. 假设有三种播种方式：A，B 和 C. 为度量不同肥料用量的效果，农夫可以按如下方法将一块地分成 9 块小地：

⊖ 若 A 是一个拉丁方，则 A 和 A^{T} 正交不是总成立的. 例如，例 3.126 中的 4×4 拉丁方 A 在主对角线上的元素都为 0，它的转置也是如此. 因为 $A\circ A^{\mathrm{T}}$ 的对角线上的所有元素都等于$(0, 0)$，所以拉丁方 A 和 A^{T} 不正交.

化肥用量	种子类型		
高	A	B	C
中	A	B	C
低	A	B	C

在每个位置观察 x_{sf}，其中 x_{sf} 是穗的数量，是根据播种方式 s 和肥料用量 f 而收获的.

现在农夫想知道杀虫剂的不同用量产生的效果. 他可能有 27 个观察结果 x_{sfp}(一般地，若有 n 个不同剂量和 n 个不同播种方式，则有 n^3 个观察结果). 另一方面，假设他按如下方式安排试验(我们说明 $n=3$ 的情形).

	杀虫剂用量		
化肥用量	高	中	低
高	A	B	C
中	C	A	B
低	B	C	A

现在播种方式安排在一个拉丁方中. 例如，西北方向那一小块地的观察结果是通过播种方式 A，肥料的高水平用量和杀虫剂的高水平用量而收获的穗的数量. 观察结果只有 9 个，而不是 27 个(一般地，观察结果有 n^2 个而不是 n^3 个). 很显然，我们不能取得所有可能的观察结果. 通过测量一小部分样本从而推断出一个大的集合的性质是统计学的任务. 而且这还表明，从本质上讲，数据的拉丁方所给出的统计信息与所有 n^3 个观察结果是一样的. 314

农夫现在想考虑一下水的用量. 我们还是说明 $n=3$ 的情形. 除了播种方式 A，B，C 以及肥料及杀虫剂的不同水平用量之外，我们设水的用量水平 有三种：$\alpha>\beta>\gamma$.

	杀虫剂用量		
化肥用量	高	中	低
高	$A\alpha$	$B\beta$	$C\gamma$
中	$C\beta$	$A\gamma$	$B\alpha$
低	$B\gamma$	$C\alpha$	$A\beta$

从西北方向那一小块地观察到的结果是通过播种方式 A，肥料的高水平用量，杀虫剂的高水平用量和水的高水平用量所收获的穗的数量. 同样，从 9 个观察结果中产生的统计数据本质上与从 81 个观察结果 x_{sfpw} 中产生的统计数据相同(一般地，观察结果是 n^2 个而不是 n^4 个). 欧拉称这些矩阵是希腊-拉丁方，因为他利用拉丁和希腊字母来描述它们. 他发明术语“拉丁方”的原因也与此相同. 如果我们能找到按如下定义的一对正交的拉丁方，则可以试验更多的变量.

定义 由 $n\times n$ 拉丁方 A_1，A_2，…，A_t 构成的集合称为一个**正交集**，若它们当中每一对

都是正交的.

引理 3.136 若 A_1，A_2，…，A_t 是由 $n\times n$ 拉丁方构成的正交集，则 $t\leqslant n-1$.

证明 不失一般性，我们可假设每个 A_ν 的元素位于 $X=\{0, 1, \cdots, n-1\}$ 中. 置换 A_1 的元素使得它的第一行是 0，1，…，$n-1$，且按此顺序排列. 由引理 3.127 知，新的矩阵 A_1'是一个拉丁方，与 A_2，…，A_t 中的每一个都正交. 置换 A_2 的元素使得它的第一行是 0，1，…，$n-1$，且按此顺序排列. 新的矩阵 A_2'是一个拉丁方，与 A_1'，A_3，…，A_t 中的每一个都正交. 如此继续下去，我们可假设每个 A_ν 的顶行都是 0，1，…，$n-1$，且按此顺序排列.

若 $\nu\neq\lambda$，则阿达马积 $A_\nu\circ A_\lambda$ 的第一行是

$$(0,0),(1,1),\cdots,(n-1,n-1).$$

我们断言 A_ν 和 A_λ 没有相同的 2，1 元素. 否则，存在 k 满足 $a_{21}^{\nu}=k=a_{21}^{\lambda}$(其中 a_{ij}^{ν} 表示 A_ν 的 ij 元素)使得

315 $$(a_{21}^{\nu},a_{21}^{\lambda})=(k,k).$$

这就与 A_ν 和 A_λ 的正交性矛盾，因为序对(k, k)已经在它们的第一行中产生. 因此，不同的 A_ν 在 2，1 位置上有不同的元素. 但是，在任意 A_ν 中，2，1 元素只有 $n-1$ 个选择，这是因为 0 已经在它的 1，1 位置上出现，所以至多存在 $n-1$ 个不同的 A_ν. ■

定义 由 $n\times n$ 拉丁方构成的一个**完全正交集**是指由 $n-1$ 个拉丁方构成的一个正交集.

定理 3.137 若 $q=p^e$，则存在由 $q-1$ 个 $q\times q$ 拉丁方构成的完全正交集.

证明 若 k 是只有 q 个元素的有限域，则存在 $q-1$ 个元素 $a\in k^\times$，所以存在 $q-1$ 个拉丁方 L_a，根据定理 3.128，其中每一对都是正交的. ■

一个拉丁方可以在不同的种类(如谷类)中试验两个变量(例如肥料和杀虫剂的用量). 一个希腊-拉丁方(即一对正交的拉丁方)可以试验另一个变量(如水的用量). 一般地，由 t 个正交拉丁方构成的集合可使我们对不同的种类试验 $t+1$ 个不同的变量.

3.9.4 射影平面

现在还有另一件事情值得我们探讨. 直到 19 世纪初期，数学家们一直都在研究透视图的问题，它是画家们在二维画布上画三维场景时产生的. 我们的眼睛看见水平线似乎是在地平线上相交，这就暗示我们应在普通平面上加上一条“无穷远处的直线”. 每条直线都平行于一条过原点 O 的直线ℓ. 对每条这样的直线，我们定义一个新的点 ω_ℓ，并构造一个新的集合

$$\mathbb{P}^2(\mathbb{R})=\mathbb{R}^2\cup H,$$

其中 $H=\{\omega_\ell:\ell$ 是过 O 的一条直线$\}$. 在$\mathbb{P}^2(\mathbb{R})$中，我们定义新的**直线**：H 是一条直线(**无穷远处的直线**，或地平线)；对$\mathbb{R}^2$ 中的每条(普通的)直线 L，定义 $L^*=L\cup\{\omega_\ell\}$，其中 ℓ 是过原点并与 L 平行的直线.

我们证明$\mathbb{P}^2(\mathbb{R})$中的每对(新)直线相交于一点. 若 $L^*=L\cup\{\omega_\ell\}$，则 $L^*\cap H=\{\omega_\ell\}$. 现在考虑 $L^*\cap M^*$，其中 $M^*=M\cup\{\omega_m\}$. 若 L 和 M 平行，则 $L\cap M=\varnothing$，$\{\omega_\ell\}=\{\omega_m\}$. 因而 $L^*\cap M^*=\{\omega_\ell\}$. 若 L 和 M 不平行，则平面上存在一点 Q 使得 $L\cap M=\{Q\}$. 因为 $\omega_\ell\neq\omega_m$，所以有 $L^*\cap M^*=\{Q\}$.

每两个不同的点 Q，$R\in\mathbb{P}^2(\mathbb{R})$确定一条直线也是成立的. 若 $Q=\omega_\ell$，$R=\omega_m$，则 Q，R 确

定 H. 若 $Q=\omega_\ell$，$R\in\mathbb{R}^2$，则 Q，R 确定过 R 且与 ℓ 平行的普通直线 L，因而 Q，R 确定 L^*. 316
最后，若 Q，$R\in\mathbb{R}^2$，则它们确定平面上的一条普通直线 L，因而它们确定新直线 L^*.

既然我们现在对有限的结构感兴趣，那就让我们用有限"平面"$k\times k$ 来代替平面$\mathbb{R}\times\mathbb{R}$，其中 k 是有 q 个元素的有限域. 我们把这个有限平面看作是加法阿贝尔群的直和. 定义**过原点 $O=(0,0)$ 的直线 ℓ** 为下述形式的子集

$$\ell=\{(ax,ay):a\in k\ \text{和}(x,y)\neq O\}.$$

一般地，定义一条**直线**为一个陪集

$$(u,v)+\ell=\{(u+ax,v+ay):a\in k\}.$$

因为 k 是有限的，所以我们可以做些计算. 平面上有 q^2 个点，且每条直线上有 q 个点. 与通常情况一样，两点确定一条直线. 称两条直线**平行**，若它们不相交. 称两条直线有相同的**方向**，若它们是平行的. 有多少个方向？每条直线是过原点的直线 ℓ 的一个陪集，它们与 ℓ 有相同的方向，但是过原点的不同直线有不同的方向，因为它们是相交的. 因此方向的数目和过原点的直线的数目相等. 存在 q^2-1 个点 $V\neq O$，每一点确定过原点的一条直线 $\ell=OV$. 因为直线 ℓ 上有 q 个点，所以 ℓ 上除 O 外还有 $q-1$ 个点，且每一个点确定 ℓ. 因此有

$$(q^2-1)/(q-1)=q+1$$

个方向. 我们把 $q+1$ 个新的点 w_ℓ 加到 $k\times k$ 上，每一个点表示一个方向，即每一个点表示过原点的一条直线 ℓ. 定义 H，**无穷远处的直线**为

$$H=\{w_\ell:\ell\ \text{是过原点的一条直线}\},$$

并定义 k 上的**射影平面**

$$\mathbb{P}^2(k)=(k\times k)\cup H.$$

定义$\mathbb{P}^2(k)$中的(射影)**直线**为 H 或 $k\times k$ 中与 ω_ℓ 相连的一条直线$(u,v)+\ell$，其中 ℓ 是过原点的直线. 于是 $|\mathbb{P}^2(k)|=q^2+q+1$，每条直线有 $q+1$ 个点，且任意两点确定唯一的一条直线. 在例 4.26 中，我们将利用线性代数给出射影平面$\mathbb{P}^2(k)$的另一种构造.

例 3.138 若 $k=\mathbb{F}_2$，则 $k\times k$ 有 4 个点：$O=(0,0)$，$a=(1,0)$，$b=(0,1)$和 $c=(1,1)$，以及 6 条直线，每条直线上有两个点，如图 3-3 所示. 317

有三组平行线：Oa 和 bc，Ob 和 ac，Oc 和 ab. 射影平面$\mathbb{P}(\mathbb{F}_2)$可通过添加新的点 ω_1，ω_2，ω_3 和强迫平行线相交来得到. 存在 7 条直线：6 条早已存在的直线(每个均被加长)和无穷远处的直线$\{\omega_1,\omega_2,\omega_3\}$，如图 3-4 所示. ◀

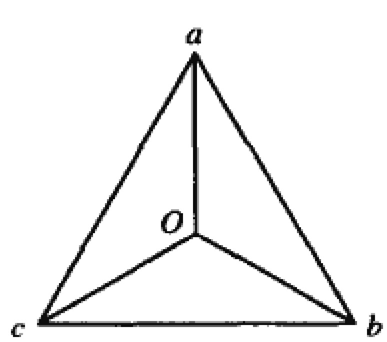


图 3-3 仿射平面

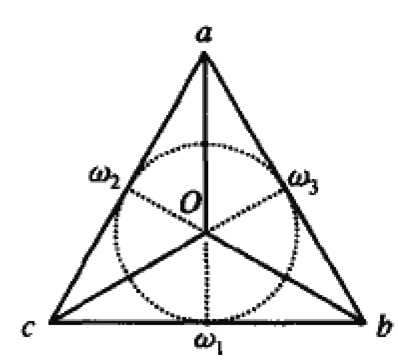


图 3-4 射影平面

现在把我们需要的图形加以抽象.

定义 阶为 n 的射影平面是指一个集合 X 满足 $|X|=n^2+n+1$，和一族称为直线的子集，每条直线上有 $n+1$ 个点，每两点确定唯一一条直线.

由上可见，若 k 是一个有限域，有 q 个元素，则$\mathbb{P}(k)$是阶为 q 的射影平面. 不用有限域也可能构造出射影平面来. 例如，已经知道存在 4 个阶为 9 的射影平面，其中只有一个是由含 9 个元素的有限域构造的.

下述定理是我们介绍射影平面的原因.

定理 若 $n\geqslant 3$，则存在阶为 n 的射影平面当且仅当存在 $n\times n$ 拉丁方构成的完全正交集.

证明 参看黎生(Ryser)的《组合数学》(Combinatorial Mathematics)第 92 页. ■

一个自然的问题是，如何求出使阶为 n 的射影平面存在的那些 n. 注意，这比欧拉的原始问题更困难些. 我们现在不是问是否存在一对正交的 $n\times n$ 拉丁方，而是问是否存在由 $n-1$ 个 $n\times n$ 拉丁方构成的正交集. 若 $n=p^e$，则我们已经构造出了阶为 n 的射影平面. 由于泰利证明
318 了不存在一对正交的 6×6 拉丁方，所以不存在 5 个两两正交的 6×6 拉丁方，所以不存在阶为 6 的射影平面. 下述定理是在 1949 年证明的.

定理(布拉克-黎生) 若 $n\equiv 1 \bmod 4$ 或 $n\equiv 2 \bmod 4$，且 n 不是两个平方数的和，则不存在阶为 n 的射影平面.

证明 参看黎生的《组合数学》第 111 页. ■

满足 $n\geqslant 3$ 的最先的 $n\equiv 1$ 或 $2 \bmod 4$ 是

$$5,\quad 6,\quad 9,\quad 10,\quad 13,\quad 14,\quad 17,\quad 18,\quad 21,\quad 22.$$

其中有一些是素数或素数的幂，所以它们一定是两个平方数的和[⊖]，因为以这些数为阶的射影平面确实存在，所以它们是

$$5=1+4;\quad 9=0+9;\quad 13=4+9;\quad 17=1+16.$$

在余下的数中，$10=1+9$ 和 $18=9+9$ 都是两个平方数的和(且不能应用这个定理)，但是其他的都不是平方数的和. 于是不存在阶为 6，14，21 和 22 的射影平面(因此泰利的结果可由布拉克-黎生定理得到).

使布拉克-黎生定理(Bruck-Ryser theorem)不能成立的最小的 n 是 $n=10$. 是否存在阶为 10 的射影平面是许多研究的课题(在泰利之后，10 也是欧拉猜想的第一个公开情形). 这是一个关于 111 个点构成的集合的问题，所以我们可以期望用计算器很快地解决它. 但它实际上它是关于一个有 111 个点的集合的 11-点子集的问题，其大小的阶数是二项式系数 $\binom{111}{11}$，一个巨大的数. 尽管如此，勒姆(C. Lam)在 1988 年证明了不存在阶为 10 的射影平面. 他利用了大量的计算：在 CRAY-1S 上花了 3000 个小时后，又在 VAX 11/780 上花了 19200 个小时. 因此，实际上用了两年半的计算时间来解决这个问题. 在写这本书的时候，我们还不知道是否存
319 在阶为 12 的射影平面($12\equiv 0 \bmod 4$，所以在布拉克-黎生定理中没有提到这个问题).

⊖ 回忆费马二平方定理(定理 3.83)：若 $p\equiv 1 \bmod 4$，则 p 是两个平方数的和. 因为存在阶为 p 的射影平面，所以布拉克-黎生定理可推出二平方定理. 实际上，布拉克-黎生定理可推出：若 $p\equiv 1 \bmod 4$，则 p^e 是两个平方数的和，其中 $e\geqslant 1$.

第4章 线性代数

→4.1 向量空间

线性代数主要研究向量空间、向量空间的同态(称之为线性变换，可用矩阵具体地描述)及它们在线性方程组方面的应用．大部分读者已经学习了含有元素为实数或复数的矩阵的有关课程，因此4.1、4.3和4.4节可以跳过，而不受影响(大部分结果，尽管建立在纯量属于任意域的向量空间上，但与向量空间是实向量空间这一特殊情形的结果有本质上相同的证明)．然而请注意，在4.2节尺-规作图的讨论中，纯量是属于$\mathbb{C}$的一个特定的子域，这个子域我们以前不熟悉，而在4.5节码理论(这些思想使得我们能看到外层空间传回来的照片)的讨论中，纯量是属于有限域的.

→ **定义** 设k是一个域，k**上向量空间**定义为一个带有如下**纯量乘法**的(加法)交换群V：即存在$k\times V\to V$的函数，记为$(a, v)\mapsto av$，使得对所有a，$b\in k$及所有u，$v\in V$，有

(i)$a(u+v)=au+av$;

(ii)$(a+b)v=av+bv$;

(iii)$(ab)v=a(bv)$;

(iv)$1v=v$，其中1是k中的单位元.

除了这5个明确提及的公理外[纯量乘法是由公理(i)～(iv)定义的]，还有几个公理以含蓄的方式表明了向量空间是一个加法交换群．加法是一个函数$V\times V\to V$，记为$(u, v)\mapsto u+v$，满足下列等式：对所有的u，v，$w\in V$，

(i)′$(u+v)+w=u+(v+w)$; 320

(ii)′$u+v=v+u$;

(iii)′存在$0\in V$，满足$0+v=v$;

(iv)′对每一个$v\in V$，存在$v'\in V$，满足$v+v'=0$.

因此，向量空间的定义包括10条公理.

V中的元素称为**向量**[⊖]，k中的元素称为**纯量**[⊜].

→ **例4.1** (i)欧氏空间$V=\mathbb{R}^n$是$\mathbb{R}$上的一个向量空间．向量是n元有序数组$v=(a_1, \cdots, a_n)$，其中对所有i有$a_i\in\mathbb{R}$．可以将向量v用从原点到坐标为$(a_1, \cdots, a_n)$的点的一个箭头表示．加法规定为

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n);$$

从几何上讲，两个向量的和由**平行四边形定律**描述(见图2-5).

若$c\in\mathbb{R}$，则由c给出的纯量乘法定义为

⊖ "向量"一词来自它的拉丁语词根，原意为"携带"的意思．在欧氏空间中，向量是"携带"长度和方向的数据.

⊜ "纯量"一词从纯量乘法$v\mapsto cv$只是将所有向量引起一个大小改变而来．术语"scalar"及"scale"来自拉丁语，意为"梯子"(ladder)．因为梯子的所有阶梯有相同间隔.

$$cv = c(a_1, \cdots, a_n) = (ca_1, \cdots, ca_n).$$

纯量乘法 $v \mapsto cv$ 将 v“拉长”了 $|c|$ 倍，当 c 为负数时，方向相反(在“拉长”上加引号是因为当 $|c|<1$ 时，cv 的长度比 v 的短).

(ii)上述(i)中的例子可以推广为更一般的情形. 设 k 为任意一个域，定义 $V=k^n$ 是所有 n 元有序组 $v=(a_1, \cdots, a_n)$ 的集合，其中对所有 i，$a_i \in k$. 除非另外说明，我们通常将 k^n 中的向量看成 $n\times 1$ 列向量. 加法和由 $c\in k$ 给出的纯量乘法像(i)中一样给出：

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n);$$

$$c(a_1, \cdots, a_n) = (ca_1, \cdots, ca_n).$$

(iii)如果 R 是一个交换环，k 是 R 的一个子环且是一个域，则 R 为 k 上的一个向量空间. 视 R 中的元素为向量，k 中的元素为纯量，规定纯量乘法 cv 就是 R 中两个元素的乘积，其中 c
321 $\in k$，$v\in R$. 注意，向量空间定义中的公理就是在交换环 R 中成立的某些公理的特殊形式.

例如，设 k 为域，则多项式环 $R=k[x]$是 k 上的一个向量空间. 向量为多项式 $f(x)$，纯量为元素 $c\in k$，纯量乘法给出多项式 $cf(x)$，即若

$$f(x) = b_n x^n + \cdots + b_1 x + b_0,$$

则

$$cf(x) = cb_n x^n + \cdots + cb_1 x + cb_0.$$

特别地，若域 k 是更大的域 E 的一个子域，则 E 为 k 上的一个向量空间. 例如，$\mathbb{C}$ 为 $\mathbb{R}$ 上的一个向量空间.

(iv)若 k 是一个域，用 $\mathrm{Mat}_{m\times n}(k)$表示所有元素在 k 中的 $m\times n$ 的矩阵构成的集合. 两个矩阵 A 和 B 的和 $A+B$ 定义为相应位置的元素相加：若 $A=[a_{ij}]$，$B=[b_{ij}]$，则

$$A + B = [a_{ij} + b_{ij}].$$

若 $c\in k$，则用 c 去乘 $A=[a_{ij}]$的每个元素给出

$$cA = [ca_{ij}].$$

使用常规的方法就可验证 $\mathrm{Mat}_{m\times n}(k)$是 k 上的一个向量空间.

若 $n=1$，则 $\mathrm{Mat}_{n\times 1}(k)=k^n$. 若 $m=n$，我们用 $\mathrm{Mat}_n(k)$来代替 $\mathrm{Mat}_{n\times n}(k)$. ◀

向量空间 V 的一个子空间是 V 的一个子集，它在 V 的加法和纯量乘法下也是一个向量空间. 然而我们给出一个更简单的定义，以便于使用.

→ **定义** 设 V 是域 k 上的一个向量空间，V 的一个子集 U 称为 V 的一个**子空间**，若有

(i)$0\in U$；

(ii)当 u，$u'\in U$ 时，$u+u'\in U$；

(iii)当 $u\in U$，$c\in k$ 时，$cu\in U$.

→ **命题 4.2** 域 k 上向量空间 V 的每一个子空间 U 本身就是域 k 上的向量空间.

证明 由假设，U 在纯量乘法下是封闭的：若 $u\in U$，$c\in k$，则 $cu\in U$. 向量空间定义中的公理(i)～(iv)对所有纯量和 V 中的所有向量均成立；特别地，对 U 中的所有向量也都成立. 例如，公理(iii)说对所有 a，$b\in k$ 和所有 $v\in V$，$(ab)v=a(bv)$成立；特别地，对所有的 $u\in U$，
322 这些等式也成立.

由假设，U 在加法下是封闭的：若 u，$u'\in U$，则 $u+u'\in U$. 向量空间定义中的公理(i)'～(iv)'对所有纯量和 V 中的所有向量都成立；特别地，对 U 中的所有向量也都成立. 最后，公理(iii)'要求 $0\in U$，这正是假设的一部分. ■

→ **例 4.3** (i)极端情形 $U=V$ 及 $U=\{0\}$(其中$\{0\}$表示仅包含零向量的子集)总是任何向量空间的子空间. 满足 $U\neq V$ 的子空间 $U\subseteq V$ 称为 V 的**真子空间**. 我们用 $U\subsetneq V$ 表示 U 为 V 的一个真子空间.

(ii)如果 $v=(a_1, \cdots, a_n)$是$\mathbb{R}^n$ 的一个非零向量，则

$$\ell=\{av : a\in \mathbb{R}\}$$

是通过原点的一条直线，且 ℓ 为$\mathbb{R}^n$ 的一个子空间. 例如，对角线$\{(a, a) : a\in\mathbb{R}\}$是平面$\mathbb{R}^2$ 的一个子空间.

类似地，通过原点的一个平面由所有形如 av_1+bv_2 的向量构成，其中 v_1，v_2 是一对固定的不共线的向量，a，b 取遍$\mathbb{R}$ 中的值. 易证，通过原点的平面也是$\mathbb{R}^n$ 的子空间.

由命题 4.2，通过原点的直线和平面都是向量空间；没有这个命题，人们就应该验证向量空间定义中的十条公理.

(iii)设 $m\leqslant n$，把$\mathbb{R}^m$ 看成$\mathbb{R}^n$ 中所有后 $n-m$ 个坐标为 0 的向量构成的集合，则$\mathbb{R}^m$ 为$\mathbb{R}^n$ 的一个子空间. 例如，我们视$\mathbb{R}^1=\mathbb{R}$ 为$\mathbb{R}^2$ 中形如$(x, 0)$的点集；也就是说，$\mathbb{R}$ 可以看成平面中的实轴.

(iv)设 k 是一个域，则 n 个未知量 m 个方程构成的 k **上的线性方程组**为

$$\begin{aligned}a_{11}x_1+\cdots+a_{1n}x_n&=b_1\\a_{21}x_1+\cdots+a_{2n}x_n&=b_2\\&\vdots\\a_{m1}x_1+\cdots+a_{mn}x_n&=b_m,\end{aligned}\qquad(1)$$

其中 a_{ij}，$b_i\in k$. 线性方程组的解是对所有的 i，满足 $\sum_j a_{ij}s_j=b_i$ 的一个向量 $s=(s_1,\cdots,s_n)\in k^n$. 所有的解构成的集合是 k^n 的一个子集，称之为此方程组的一个**解集**. 如果线性方程组无解，则称此方程组是**不相容的**. 若所有 b_i 都为 0，则称线性方程组为**齐次的**. 因为零向量一定是齐次线性方程组的一个解，故齐次线性方程组总是相容的. 用矩阵记号的话，这些定义可写得更紧凑. 方程组(1)的**系数矩阵**为 $A=[a_{ij}]$. 若 b 表示列向量$(b_1, \cdots, b_m)$，则 $s=(s_1, \cdots, s_n)$ 323
是一个解当且仅当 $As=b$. 齐次方程组 $Ax=0$ 的一个解 s 称为**非平凡的**，若有某些 $s_j\neq 0$.

一个齐次线性方程组的所有解的集合构成 k^n 的一个子空间，称为方程组的**解空间**(或零空间). 为此，设 $Ax=0$ 为一个齐次方程组，U 为它的解空间. 因为 $A0=0$，故 $0\in U$. 若 u，$u'\in U$,则 $Au=0=Au'$，因此 $A(u+u')=Au+Au'=0+0=0$，所以 $u+u'\in U$. 若 $c\in k$，$u\in U$，则 $A(cu)=c(Au)=c0=0$，所以 $cu\in U$. 从而 U 是 k^n 的一个子空间.

我们可以求解域$\mathbb{F}_p$ 上的线性方程组，其中 p 是一个素数. 这就是说，我们可以像处理普通的线性方程组一样来处理模 p 的同余方程组.

例如，同余方程组

$$3x-2y+z\equiv 1 \bmod 7$$

$$x+y-2z\equiv 0 \bmod 7$$
$$-x+2y+z\equiv 4 \bmod 7$$

可以看成域$\mathbb{F}_7$上的线性方程组. 因为元素在模 7 下的逆是已知的：[2][4]=[1]，[3][5]=[1]，[6][6]=[1]，所以此方程组只需用中学所学的方法求解即可. 它的解为

$$(x,y,z)=([5],[4],[1]).$$

(v)回忆 $m\times n$ 矩阵 $A=[a_{ij}]$的**转置**是 $n\times m$ 矩阵 A^{T}，它的 ij 元素是 a_{ji}；A 的第 i 行是 A^{T} 的第 j 列，A 的第 j 列是 A^{T} 的第 j 行. 转置的基本性质是

$$(A+B)^{\mathrm{T}}=A^{\mathrm{T}}+B^{\mathrm{T}};\quad (cA)^{\mathrm{T}}=cA^{\mathrm{T}};$$
$$(AB)^{\mathrm{T}}=B^{\mathrm{T}}A^{\mathrm{T}};\quad (A^{\mathrm{T}})^{\mathrm{T}}=A.$$

$n\times n$ 矩阵 A 是**对称的**，若 $A^{\mathrm{T}}=A$. 若 k 是一个域，我们来证明所有对称的 $n\times n$ 矩阵组成的集合 S 是 $\mathrm{Mat}_n(k)$的一个子空间. 用 0 来表示所有元素都是 0 的矩阵，则 $0^{\mathrm{T}}=0$，故 $0\in S$. 若 A，$B\in S$，则

$$(A+B)^{\mathrm{T}}=A^{\mathrm{T}}+B^{\mathrm{T}}=A+B,$$

故 $A+B\in S$. 最后，若 $c\in k$，$A\in S$，则

$$(cA)^{\mathrm{T}}=c(A)^{\mathrm{T}}=cA,$$

故 $cA\in S$. 因此 S 是 $\mathrm{Mat}_n(k)$的一个子空间. 由命题 4.2 可知，元素在一个域 k 中的所有 $n\times n$

324 对称矩阵组成的集合是一个向量空间. ◀

下面的方阵是重要的.

→ **定义** 称一个 $m\times m$ 矩阵 A 是**非奇异的**，若存在一个 $m\times m$ 矩阵 B 使得 $AB=I$ 且 $BA=I$. B 称为 A 的**逆**，记为 A^{-1}.

回忆$\mathbb{R}^3$ 中两个向量 $v=(a,\ b,\ c)$，$v'=(a',\ b',\ c')$的**点积**定义为 $v\cdot v'=aa'+bb'+cc'\in\mathbb{R}$. 这个数有一个几何解释：

$$v\cdot v'=\|v\|\ \|v'\|\cos\theta,$$

其中 $\|v\|$ 是 v 的长度，θ 是 v 和 v'间的夹角. 由此得出，若 $v\cdot v'=0$，则 $v=0$，$v'=0$ 或者 v 和 v'是**正交的**⊖. 我们可改进点积的定义以适应更一般的空间.

→ **定义** 设 k 是一个域，V 是 k 上的一个向量空间，则 V 上的一个**内积**是一个函数 $f:V\times V\to k$，通常记为 $f(v,\ w)=(v,\ w)$，满足：

(i) $(v,\ w+w')=(v,\ w)+(v,\ w')$，对所有的 v，w，$w'\in V$；

(ii) $(v,\ aw)=a(v,\ w)$，对所有的 v，$w\in V$，$a\in k$；

(iii) $(v,\ w)=(w,\ v)$，对所有的 v，$w\in V$.

一个内积称为**非退化的**(或**非奇异的**)，若对所有的 $v\in V$，$(v,\ v)=0$ 能推出 $v=0$.（此定义的一个应用，可参阅定理 4.104.）

→ **例 4.4** (i)设 k 是任一个域，$V=k^n$，且令 $v=(a_1,\ \cdots,\ a_n)$，$v'=(a_1',\ \cdots,\ a_n')\in V$，则

$$(v,v')=a_1a_1'+\cdots+a_na_n'$$

⊖ 原词为 orthogonal. 在希腊语中，"ortho"意思为"垂直的"，"gon"意思为"角"，因此"orthogonal"意思为"直角的"或"正交的".

是 k^n 上的一个内积. 若 $k=\mathbb{R}$，则此内积是非退化的，因为若 $\sum_i a_i^2=0$，则每一个 $a_i=0$. 然而，若 $k=\mathbb{C}$，则此内积是**退化的**(不是非退化的). 例如，设 $n=2$，$v=(1, i)$，则 $(v, v)=1+i^2=0$. 对向量空间 $V=\mathbb{C}^n$ 来说，人们通常将它修改为 $(v, v')=\sum a_j \bar{a}_j'$，其中 $\bar{a}$ 是复共轭. 这并未给出一个内积[因为定义中的公理(ii)可能不成立：$(v, aw)=\bar{a}(v, w)$]，但它使得由 $(v, v)=0$ 可推出 $v=0$.

在定义于有限域 k 上的向量空间上的内积中，同样的现象也会出现. 例如，设 $k=\mathbb{F}_2$，若 n 是偶数，$v=(1, \cdots, 1)\in k^n$，则 $(v, v)=0$；若 n 是奇数，$v=(0, 1, \cdots, 1)$，则 $(v, v)=0$. 325

(ii) 设 k 是一个域，视 k^n 中的向量为 $n\times 1$ 列矩阵. 若 A 是元素在 k 中的 $n\times n$ 对称矩阵，定义 $V=k^n$ 上的内积为

$$(v,w)=v^{\mathrm{T}}Aw.$$

读者可以证明，这是一个内积，且它是非退化的当且仅当 A 是一个非奇异的矩阵. ◀

→ **例 4.5** 设 V 是一个带有一个内积的向量空间，设 $W\subseteq V$ 是一个子空间. 定义

$$W^{\perp}=\{v\in V:(w,v)=0,\text{对所有的 } w\in W\}.$$

我们来验证 $W^{\perp}$(读成 W 垂)是一个子空间. 显然，$0\in W^{\perp}$. 若 $v, v'\in W^{\perp}$，则 $(w, v)=0$，$(w, v')=0$，对所有的 $w\in W$，因此 $(w, v+v')=(w, v)+(w, v')=0$，对所有的 $w\in W$，因此 $v+v'\in W^{\perp}$. 最后，若 $v\in W^{\perp}$ 且 $a\in k$，则 $(w, av)=a(w, v)=0$，故 $av\in W^{\perp}$. 因此 $W^{\perp}$ 是的一个子空间，它被称为 W 的**正交补**. 需要提醒大家的是，在欧氏空间中，$(v, w)=0$ 的确推出 v 和 w 是正交的向量. 易见，$W\cap W^{\perp}=\{0\}$ 当且仅当内积是非退化的. ◀

维数是一个相当难以理解的概念. 让我们考虑平面上的一条曲线，即连续函数 $f: \mathbb{R}\to\mathbb{R}^2$ 的图像，它是二维环绕空间上的一维子集. 想象一下 19 世纪末期认识上的混乱吧，人们当时发现"填满了空间的曲线"：存在一个连续函数 $f: \mathbb{R}\to\mathbb{R}^2$ 使得 f 的图像为整个平面！我们现在来描述在向量空间中定义维数的一种方式，这与欧氏空间中的方式一样(在更一般的空间中定义维数有拓扑的方式).

获得"合适"的维数定义的关键在于理解 $\mathbb{R}^3$ 为什么是三维的. 每个向量 (x, y, z) 都是 3 个向量 $e_1=(1, 0, 0)$，$e_2=(0, 1, 0)$，$e_3=(0, 0, 1)$ 的线性组合，即

$$(x,y,z)=xe_1+ye_2+ze_3.$$

每个向量都是这些特定向量的线性组合并不重要，重要的是这些特定向量只有 3 个，因为可以证明，3 是 $\mathbb{R}^3$ 中具有每个向量都是它们的线性组合这一性质的向量的最小个数.

→ **定义** *向量空间 V 中的一个***表**[⊖]*指的是 V 中的一组有序向量 $X=v_1, \cdots, v_n$，其中 $n\in\mathbb{N}$. 特别地，我们允许不含向量的***空表***(它是 $n=0$ 时的表).* 326

更准确地，我们是说 V 中的一个表是一个函数：

$$\varphi:\{1,2,\cdots,n\}\to V,$$

对 $n\in\mathbb{N}$，满足对所有 i 有 $\varphi(i)=v_i$. 注意 X 在这个意义下是排了序的：第一个向量是 v_1，第

⊖ 一个表 $X=a_1, \cdots, a_n$ 准确地说，就是一个 n 元有序元素组 $(a_1, \cdots, a_n)$，我们用括号来记 n 元有序元素组是为了与标准的记号保持一致.

二个向量是 v_2，等等．一个向量可以在一个表中出现多次，即 φ 不必是单射．空表 φ 满足性质 $\mathrm{im}\varphi=\varnothing$.

→ **定义** 设 V 是域 k 上的一个向量空间．V 中一个非空的表 v_1，…，v_n 的一个**线性组合**指的是如下形式的向量 v：

$$v = a_1v_1 + \cdots + a_nv_n,$$

其中 $n\in\mathbb{N}$ 且对所有 i 有 $a_i\in k$．空表的线性组合定义为 0，零向量.

→ **定义** 如果 $X=v_1$，…，v_m 为向量空间 V 的一个表，则

$$\langle X\rangle = \langle v_1,\cdots,v_m\rangle,$$

表示 v_1，…，v_m 的所有线性组合构成的集合，称为由 X **生成的子空间**，我们也称 v_1，…，v_m **张成** $\langle v_1, \cdots, v_m\rangle$.

例 4.6 设 A 是域 k 上的一个 $m\times n$ 的矩阵，则它的**行空间** $Row(A)$ 是由 A 的行向量生成的 k^n 的子空间．A 的**列空间** $Col(A)$ 是由 A 的列向量生成的 k^m 的子空间．注意 $Row(A)=Col(A^T)$，$Col(A)=Row(A^T)$，因为 A 的列就是 A^T 的行(且 A 的行是 A^T 的列).

若 A 是一个 $m\times n$ 矩阵，它的行空间 $Row(A)$，列空间 $Col(A)$ 及 $Ax=0$ 的**解空间** $Sol(A)$ 是相关连的．若 k^n 上的内积是非退化的，则 $Row(A)^{\perp}=Sol(A)$，$Col(A)^{\perp}=Sol(A^T)$，且 $Sol(A)^{\perp}=Row(A)$（见雷恩（Leon）所著的《线性代数及应用》(Linear Algebra with Applications)，第 242～244 页). ◀

→ **命题 4.7** 设 $X=v_1$，…，v_m 是向量空间 V 的一个表，则 $\langle X\rangle$ 是 V 的包含子集 $\{v_1, \cdots, v_m\}$ 的子空间.

证明 我们记 $L=\langle v_1, \cdots, v_m\rangle$．这样 $0\in L$，因为

$$0 = 0v_1 + \cdots + 0v_m.$$

若 $u=a_1v_1+\cdots+a_mv_m\in L$ 和 $v=b_1v_1+\cdots+b_mv_m\in L$，则

$$\begin{aligned} u+v &= a_1v_1 + \cdots + a_mv_m + b_1v_1 + \cdots + b_mv_m \\ &= a_1v_1 + b_1v_1 + \cdots + a_mv_m + b_mv_m \\ &= (a_1+b_1)v_1 + \cdots + (a_m+b_m)v_m \in L. \end{aligned}$$

327

最后，若 $c\in k$，则

$$c(a_1v_1 + \cdots + a_mv_m) = (ca_1)v_1 + \cdots + (ca_m)v_m \in L.$$

因此，L 是一个子空间.

为证每个 $v_i\in L$，只需选择 $a_i=1$ 和其余系数全为 0 的线性组合. ■

设 $X=v_1$，…，v_m 是向量空间 V 的一个表，则它的**基础集**是子集 $\{v_1, \cdots, v_m\}$．注意到 v_1，v_2，v_3 和 v_2，v_1，v_3 是两个不同的表，但具有相同的基础集．更进一步，v_1，v_2，v_2 和 v_1，v_2 也是两个不同的表，但具有相同的基础集．我们对表及基础集的细节如此注意的一个原因可以在 4.1 节中的坐标的讨论中找到.

引理 4.8 若 $X=v_1$，…，v_n 是向量空间 V 的一个表，则 $\langle X\rangle$ 只依赖它的基础集 $\{v_1, \cdots, v_m\}$.

证明 设 $\sigma\in S_n$ 是一个置换，则定义一个表 $X^{\sigma}=v_{\sigma(1)}$，…，$v_{\sigma(n)}$．X 的一个线性组合是一个向量 $v=a_1v_1+\cdots+a_nv_n$．因为 V 中的加法是交换的，所以 X 也是表 X^{σ} 的一个线性组合.

因此$\langle X\rangle=\langle X^{e}\rangle$，因为两个子集是由一样的向量构成的.

如果表 X 有重复的元素，如 $v_i=v_j$，对 $i\neq j$，则

$$a_1v_1+\cdots+a_nv_n=a_1v_1+\cdots+(a_i+a_j)v_i+\cdots+\hat{v}_j+\cdots+a_nv_n,$$

其中 $a_1v_1+\cdots+\hat{v}_j+\cdots+a_nv_n$ 表示除去 v_j 后更短的和式. 由此得出 X 的线性组合构成的集合与从 X 中去除 v_j 后更短的表的线性组合构成的集合是一样的. ■

我们现在将$\langle Y\rangle$的定义推广至任意的，有可能是无限的，子集 $Y\subseteq V$.

→ **定义** 设 Y 是向量空间 V 的一个子集，则$\langle Y\rangle$是表 v_1，…，v_n 的所有有限线性组合构成的集合，其中 $n\in\mathbb{N}$，表的元素都在 Y 中.

若 Y 是有限的，则引理 4.8 表明此定义与我们以前在 4.1 节中的定义是一致的.

→ **引理 4.9** 设 V 是域 k 上的一个向量空间.

(i)V 的子空间的交还是一个子空间.

(ii)如果 Y 为 V 中的一个子集，则$\langle Y\rangle$是 V 的包含 Y 的所有子空间的交.

(iii)如果 Y 为 V 中的一个子集，则$\langle Y\rangle$是 V 的包含 Y 的最小子空间；即，若 U 是 V 的任一个包含 Y 的子空间，则$\langle Y\rangle\subseteq U$. 328

证明 (i)设$\mathcal{S}$为 V 的一族子空间，记 $\bigcap_{S\in\mathcal{S}}S$ 为 W. 因为对每一个 $S\in\mathcal{S}$，$0\in S$，故 $0\in W$. 如果 x，$y\in W$，则对每一个 $S\in\mathcal{S}$，x，$y\in S$，因为 S 是一个子空间，故 $x+y\in S$，从而 $x+y\in W$. 最后，如果 $x\in W$，则对每一个 $S\in\mathcal{S}$，$x\in S$，若 $c\in k$，则对每一个 S，$cx\in S$，故 $cx\in W$. 因此 W 为 V 的一个子空间.

(ii)用$\mathcal{S}'$表示 V 的包含子集 Y 的所有子空间构成的集合，我们断言

$$\langle Y\rangle=\bigcap_{S\in\mathcal{S}'}S.$$

包含关系$\subseteq$是显然的：若 v_1，…，v_n 是一个表，其中 $v_i\in Y$ 且 $\sum_i c_iv_i\in\langle Y\rangle$，则对每一个 $S\in\mathcal{S}'$，$\sum_i c_iv_i\in S$，因为子空间包含由它的向量构成的表的所有线性组合[此论断甚至当 $Y=\varnothing$ 时也成立，因为那样的话$\langle Y\rangle=\{0\}$]. 反包含关系由一个关于交的更一般的事实可得：对任意 $S_0\in\mathcal{S}'$，我们有 $\bigcap_{S\in\mathcal{S}'}S\subseteq S_0$. 特别地，由命题 4.7 可得 $S_0=\langle Y\rangle\in\mathcal{S}'$.

(iii)包含 Y 的一个子空间 U 是在交 $\langle Y\rangle=\bigcap_{S\in\mathcal{S}'}S$ 中涉及的子空间 S 中的一个. ■

如果代数中所有术语一致，我们将称子空间$\langle Y\rangle$由 Y 生成. 用不同的术语的原因在于群论、环论与向量空间的理论是彼此独立地发展起来的.

→ **例 4.10** (i)设 $V=\mathbb{R}^2$，$e_1=(1,0)$，$e_2=(0,1)$，则 $V=\langle e_1,e_2\rangle$，因为若 $v=(a,b)\in V$，则

$$\begin{aligned}v&=(a,0)+(0,b)\\&=a(1,0)+b(0,1)\\&=ae_1+be_2\in\langle e_1,e_2\rangle.\end{aligned}$$

(ii)若 k 为一个域，$V=k^n$. 定义 e_i 是第 i 个坐标为 1，其余为 0 的 n 元有序元素组. 读者可改写(i)中的论断证明 e_1，e_2，…，e_n 生成 k^n. 表 e_1，e_2，…，e_n 称为 k^n 的**标准基**. k^n 中每

一个向量都是此标准基的一个线性组合：$(a_1, \cdots, a_n)=a_1e_1+\cdots+a_ne_n$.

(iii)向量空间 V 不一定是由一个有限序列的向量生成的. 例如，设 $V=k[x]$. 又设 $X=f_1(x), \cdots, f_m(x)$为 V 中的任一个有限表. 若 d 为这些 $f_i(x)$的最高次数，则每个(非零)线性组合 $\sum_i a_if_i(x)$的次数最高为 d，其中 $a_i\in k$. 因此 x^{d+1}就不是 X 中向量的一个线性组合，从而 X 不能生成 $k[x]$. ◀

329 尽管我们还没有定义维数，但下列定义仍然是有意义的.

→ **定义** 一个向量空间 V 称为是**有限维的**，如果它是由一个有限集生成的，否则称 V 为**无限维的**.

例 4.10(ii)表明 k^n 是有限维的，而此例的第(iii)部分表明 $k[x]$是无限维的. 由例 4.1(iii)，$\mathbb{R}$，$\mathbb{C}$ 都是$\mathbb{Q}$上的向量空间，可以证明每一个都是无限维的.

给定向量空间 V 的一个子空间 U，我们来寻找能生成 U 的表. 注意可以有许多这样的表，例如，如果 $X=v_1, \cdots, v_m$ 能生成 U，u 为 U 中的任一个向量，则 $v_1, \cdots, v_m, u$ 也能生成 U. 因此我们来寻找能生成 U 的**最短**的表.

→ **定义** 向量空间 V 的一个表 $X=v_1, \cdots, v_m$ 称为是一个**最短扩张表(或最小扩张表)**，若没有真子表 $v_1, \cdots, \hat{v}_i, \cdots, v_m$ 能生成$\langle v_1, \cdots, v_m\rangle\subseteq V$.

→ **命题 4.11** 设 V 是一个向量空间，则下列关于生成 V 的一个表 $X=v_1, \cdots, v_m$ 的条件是等价的：

(i)X 不是一个最短生成表；即，有一个真子表能生成$\langle X\rangle$.

(ii)存在 v_i 使得 v_i 属于由其余向量生成的子空间，即

$$v_i \in \langle v_1, \cdots, \hat{v}_i, \cdots, v_m\rangle;$$

(iii)存在不全为零的纯量 $a_1, \cdots, a_m$ 使得

$$\sum_{j=1}^{m} a_jv_j = 0.$$

证明 (i)⇒(ii)如果 X 不是一个最短生成表，则 X 中某一个向量，如 v_i，可以在 X 中划去，所以 $v_i\in\langle v_1, \cdots, \hat{v}_i, \cdots, v_m\rangle$.

(ii)⇒(iii)若 $v_i=\sum_{j\neq i} c_jv_j$，则假设 $a_i=-1\neq 0$，$a_j=c_j$，对所有的 $j\neq i$.

(iii)⇒(i)给定的等式可以推出这些向量中的某一个，如 v_i，是其余向量的一个线性组合，如

$$v_i =-\sum_{j\neq i} a_i^{-1}a_jv_j.$$

去除 v_i 给出一个更短的表，它仍然能生成：若 $v\in V$，则我们知道 $v=\sum_{j=1}^{m} b_jv_j$，因为表 $v_1, \cdots, v_m$ 能张成 V. 我们将 v 重新表示如下

$$\begin{aligned} v &= b_iv_i + \sum_{j\neq i} b_jv_j \\ &=-b_i\Big(\sum_{j\neq i} a_i^{-1}a_jv_j\Big) + \sum_{j\neq i} b_jv_j \in \langle v_1, \cdots, \hat{v}_i, \cdots, v_m\rangle. \end{aligned}$$

330 ■

→ **定义** 向量空间 V 的一个表 $X=v_1$，…，v_m 称为是**线性相关的**，如果存在不全为零的纯量 a_1，…，a_m 使得 $\sum_{j=1}^{m} a_j v_j=0$；否则称 X 为**线性无关的**.

空集 $\varnothing$ 规定为线性无关的(我们可以将 $\varnothing$ 解释为长度是 0 的表).

→ **例 4.12** (i)任何包含零向量的表 $X=v_1$，…，v_m 都是线性相关的.

(ii)长度为 1 的表 v_1 是线性相关的当且仅当 $v_1=0$. 因此长度为 1 的表 v_1 是线性无关的当且仅当 $v_1\neq 0$.

(iii)表 v_1，v_2 是线性相关的当且仅当其中一个向量是另一个的纯量倍.

(iv)如果表 v_1，…，v_m 中有相同的向量(也就是，$v_i=v_j$，对某些 $i\neq j$)，则 v_1，…，v_m 是线性相关的：可令 $c_i=1$，$c_j=-1$，其余的 c 为零. 因此如果 v_1，…，v_m 为线性无关的，则所有向量 v_i 是互不相同的. ◀

命题 4.11 的逆否命题是值得一提的.

→ **推论 4.13** 假设 $X=v_1$，…，v_m 是生成向量空间 V 的一个表. 则 X 是 V 的一个最短扩张表当且仅当 X 是线性无关的.

线性无关是间接定义的：不线性相关. 由于线性无关的重要性，因此我们来直接定义它. 一个表 $X=v_1$，…，v_m 称为**线性无关的**，如果当线性组合 $\sum_{j=1}^{m} a_j v_j=0$ 时，则有每一个 $a_j=0$. 通俗地说，线性无关的表的每一个"子表"本身为线性无关的(这也是将 $\varnothing$ 规定为线性无关的原因之一).

我们现在可以给出我们一直在寻找的一个概念.

→ **定义** 有限维向量空间 V 的一组**基**是一个线性无关的且能生成 V 的表.

因此，基是生成 V 的最短生成表. 当然，由例 4.12(iv)可知，在一个线性无关的表 v_1，…，v_m 中，所有向量是互不相同的.

→ **例 4.14** 在例 4.10(ii)中，我们看到标准基 $E=e_1$，…，e_n 生成 k^n，这里 e_i 是第 i 个分量为 1，其余为 0 的 n 元有序元素组. 下面我们来证明 E 是线性无关的. 注意到 $\sum_{i=1}^{n} a_i e_i=(a_1,\cdots,a_n)$，所以 $\sum_{i=1}^{n} a_i e_i=0$ 当且仅当每一个 $a_i=0$. 从而 E 为 k^n 的一组基. ◀ 331

→ **命题 4.15** 设 $X=v_1$，…，v_n 是域 k 上的向量空间 V 的一个表. 那么 X 是 V 的一组基当且仅当 V 的每一个向量都可以唯一表示为 X 中向量的一个线性组合.

证明 如果有一个向量 $v=\sum a_i v_i=\sum b_i v_i$，则 $\sum(a_i-b_i)v_i=0$. 因此 X 的线性无关性就给出对所有的 i 有 $a_i=b_i$，即表示法唯一.

反过来，表示的存在性表明由 v_i 组成的表能张成 V. 进一步，若有 $0=\sum c_i v_i$，其中 $c_i\neq 0$，则 0 作为这些 v_i 的线性组合的表示就有两个不同的方式. ■

→ **定义** 如果 $X=v_1$，…，v_n 为向量空间 V 的一组基，$v\in V$，则存在唯一一组纯量 a_1，…，a_n 使得 $v=\sum_{i=1}^{n} a_i v_i$. 这个 n 元有序组 $(a_1,\cdots,a_n)$ 称为向量 $v\in V$ 关于基 X 的**坐标表**.

若 $E=e_1, \cdots, e_n$ 为 $V=k^n$ 的标准基，则每一个向量 $v\in V$ 有唯一的表示

$$v = a_1e_1 + a_2e_2 + \cdots + a_ne_n,$$

其中对所有的 i 有 $a_i\in k$. $v\in k^n$ 的坐标表与通常的坐标一致，因为

$$v = (a_1,\cdots,a_n) = a_1e_1 + \cdots + a_ne_n.$$

因为第一个向量是 e_1，第二个向量是 e_2，一直下去，因此这个线性组合的系数确定了唯一的一组 n 元有序组$(a_1, a_2, \cdots, a_n)$. 如果 V 的一组基仅仅是 V 的一个子集，而不是一个表，则对任一个向量我们将有 $n!$ 组坐标表与之对应.

我们接着要把向量空间的维数定义为基中向量的个数. 这样就会立即出现两个问题：

(i)每个向量空间都有基吗？

(ii)向量空间的所有的基所含向量的个数都相同吗？

第一个问题很容易回答，第二个要费一点事.

→ **定理 4.16** 每一个有限维向量空间 V 都有基.

证明 因为 V 是有限维的，存在一个有限的扩张表 X. 如果它是线性无关的，则它为一组基. 否则由命题 4.11 知，X 可缩短为一个扩张子表 X'. 若 X'是线性无关的，则它为一组基；若不是，X'可缩短为一个扩张子表 X''. 最终我们可得到一个最短扩张子表，它是线性无关的，因此它是一组基. ■

332

注 张成、线性无关性等概念可以推广至无限维向量空间(当处理无限维向量空间时，人们通常是说子集张成子空间，而不是说由表张成)，我们可以证明这些向量空间也有基. 例如，下列就是 $k[x]$的一组基：$1, x, x^2, \cdots, x^n, \cdots$. ◀

我们来证明维数的不变性，这是向量空间中最重要的结果之一.

→ **引理 4.17** 设 $u_1, \cdots, u_n$ 张成向量空间 V. 若 $v_1, \cdots, v_m\in V$ 且 $m>n$，则 $v_1, \cdots, v_m$ 是一个线性相关的表.

证明 对 $n\geqslant 1$ 归纳来证明.

基础步骤. 若 $n=1$，则存在至少两个向量 v_1, v_2，因为 $m>n$，且 $v_1=a_1u_1$，$v_2=a_2u_1$. 若 $u_1=0$，则 $v_1=0$，因此由这些 v 构成的表是线性相关的. 设 $u_1\neq 0$，我们也可假设 $v_1\neq 0$，否则我们已证毕. 因此 $a_1\neq 0$，从而 $u_1=a_1^{-1}v_1$，所以 v_1, v_2 是线性相关的(因为 $v_2-a_2a_1^{-1}v_1=0$)，从而更大的表 $v_1, \cdots, v_m$ 是线性相关的.

归纳步骤. 对 $i=1, \cdots, m$，存在等式，

$$v_i = a_{i1}u_1 + \cdots + a_{in}u_n.$$

我们可假设某些 $a_{i1}\neq 0$，否则 $v_1, \cdots, v_m\in\langle u_2, \cdots, u_n\rangle$，应用归纳假设即得证. 必要时改变记号(即重新对这些 v 排序)，我们可假设 $a_{11}\neq 0$. 对每一个 $i\geqslant 2$，定义

$$v_i' = v_i - a_{i1}a_{11}^{-1}v_1 \in \langle u_2,\cdots,u_n\rangle.$$

因为在 v_i'的表达式中，u_1 的系数为 $a_{i1}-(a_{i1}a_{11}^{-1})a_{11}=0$. 因为 $m-1>n-1$，由归纳假设，存在不全为 0 的纯量 $b_2, \cdots, b_m$ 使得

$$b_2v_2' + \cdots + b_mv_m' = 0.$$

用 v_i'的定义重写以上等式：

$$\left(-\sum_{i\geqslant 2} b_i a_{i1} a_{11}^{-1}\right) v_1 + b_2 v_2 + \cdots + b_m v_m = 0.$$

并不是所有的系数都是 0，因此 v_1，…，v_m 是线性相关的. ■ 333

→ **定理 4.18(维数不变性)** 如果 $X=x_1, x_2, \cdots, x_n$ 和 $Y=y_1, y_2, \cdots, y_m$ 为向量空间 V 的两组基，则 $m=n$.

证明 若 $m\neq n$，则或者 $n<m$，或者 $m<n$. 在第一种情形下，$y_1, y_2, \cdots, y_m\in\langle x_1, x_2, \cdots, x_n\rangle$，因为 X 张成 V. 引理 4.17 给出 Y 是线性相关的，矛盾！当 $m<n$ 时，类似的矛盾同样出现了，因此我们必有 $m=n$. ■

现在允许我们作如下定义.

→ **定义** 如果 V 是域 k 上的一个有限维向量空间，则它的**维数**，记为 $\dim(V)$，规定为 V 的任意一个基中元素的个数.

→ **例 4.19** (i)例 4.14 表明 k^n 的维数为 n，因为标准基中有 n 个元素，与 $k=\mathbb{R}$ 时我们的直觉相符. 因此平面 $\mathbb{R}\times\mathbb{R}$ 是 2 维的！

(ii)如果 $V=\{0\}$，则 $\dim(V)=0$. 因为在它的基 $\varnothing$ 中没有任何元素.（这也是定义 $\varnothing$ 线性无关的原因.）

(iii)设 $X=\{x_1, \cdots, x_n\}$ 为一个有限集. 定义

$$k^X = \{\text{函数 } f: X\to k\}.$$

若我们规定加法 $f+f'$ 为

$$f+f': x\mapsto f(x)+f'(x),$$

纯量乘法 af 为

$$af: x\mapsto af(x),$$

其中 $a\in k$，$f: X\to k$，则 k^X 为一个向量空间.

易证，下面规定的 n 个函数 f_x，$x\in X$，

$$f_x(y)=\begin{cases}1, & \text{若 } y=x;\\ 0, & \text{若 } y\neq x,\end{cases}$$

为 k^X 的一组基，从而 $\dim(k^X)=n=|X|$.

这不是一个新的例子：首先，一个 n 元有序元素组 $(a_1, \cdots, a_n)$ 实际上就是一个满足 $f(i)=a_i$（对所有 i）的函数 $f:\{1, 2, \cdots, n\}\to k$. 因此，函数 f_x 构成了标准基. ◀

下面的证明说明了线性代数和线性方程组之间的密切关系. 334

推论 4.20 一个域 k 上的齐次线性方程组，若它的未知量的个数多于方程的个数，则它一定有非平凡的解.

证明 一个 n 元有序元素组 $(s_1, \cdots, s_n)$，若对所有的 i，有 $a_{i1}s_1+\cdots+a_{in}s_n=0$，则它是下面方程组的解

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0\\ \vdots \qquad \vdots \qquad &\vdots\\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0\end{aligned}$$

换言之，若 C_1，…，C_n 为 $m\times n$ 的系数矩阵 $A=[a_{ij}]$ 的列向量，则由矩阵的乘法，有

$$s_1C_1+\cdots+s_nC_n=0.$$

注意到 $C_i\in k^m$，而 k^m 可由 m 个向量(如，标准基)扩张. 因为由假设 $n>m$，故引理 4.17 表明表 C_1，…，C_n 是线性相关的，因此存在不全为零的纯量 p_1，…，p_n 使得 $p_1C_1+\cdots+p_nC_n=0$，因此 $(p_1,\cdots,p_n)$ 为此方程组的一个非平凡的解. ■

→ **定义** 称向量空间 V 中的一个表 u_1，…，u_m 为一个**最长的线性无关表**(或者一个**极大的线性无关表**)，如果不存在 $v\in V$ 使得 u_1，…，u_m，v 为线性无关的.

→ **引理 4.21** 设 V 是一个有限维的向量空间.

(i) 设 v_1，…，v_m 为 V 中的一个线性无关的表，并设 $v\in V$. 若 $v\notin\langle v_1,\cdots,v_m\rangle$，则 v_1，…，v_m，v 是线性无关的.

(ii) 若最长的线性无关表 $X=v_1$，…，v_n 存在，则它为 V 的一组基. 反之，若一组基存在，则它就是一个最长的线性无关表.

证明 (i) 设 $av+\sum_i a_iv_i=0$. 若 $a\neq 0$，则 $v=-a^{-1}\sum_i a_iv_i\in\langle v_1,\cdots,v_m\rangle$，矛盾. 因此 $a=0$ 且 $\sum_i a_iv_i=0$. 由 v_1，…，v_m 的线性无关性即可推出每一个 $a_i=0$，所以更长的表 v_1，…，v_m，v 是线性无关的.

(ii) 若 X 不是一个组基，则它不能扩张成 V：存在 $w\in V$ 使得 $w\notin\langle v_1,\cdots,v_n\rangle$. 但由(i)知，更长的表 X，w 为线性无关的，从而与 X 是一个最长的线性无关表相矛盾. 请读者证其余部分. ■

当然最长的线性无关表的存在性不明显，但从下面这个结果可得出它们的确是存在的，并
335 且此结果本身也相当有用.

→ **命题 4.22** 设 V 为一个 n 维向量空间，$Z=u_1$，…，u_m 为 V 的一个线性无关的表，则 Z 可以扩充为 V 的一组基，也就是，存在向量 v_1，…，v_{n-m} 使得 u_1，…，u_m，v_1，…，v_{n-m} 为 V 的一组基.

证明 若 $m>n$，则由引理 4.17 可推出 Z 是线性相关的，矛盾，因此 $m\leqslant n$. 若此线性无关的表 Z 不能生成 V，则存在 $v_1\in V$ 使得 $v_1\notin\langle Z\rangle$，且由引理 4.21，更长的表 Z，$v_1=u_1$，…，u_m，v_1 是线性无关的. 若 Z，v_1 不能生成 V，则存在 $v_2\in V$ 使得 $v_2\notin\langle Z, v_1\rangle$. 此个过程最终会停止，因为这些表的长度不可能超过 $n=\dim(V)$. ■

→ **推论 4.23** 若 $\dim(V)=n$，则 V 的任何长为 $n+1$ 的表均为线性相关的.

证明 否则，这样的表能扩充为一组基，而此基的元素个数超过了 n. ■

在练习题 4.11 中我们已经证明了，若 $\mathrm{Mat}_{m\times n}(k)$ 是 k 上的所有 $m\times n$ 矩阵构成的向量空间，则 $\dim(\mathrm{Mat}_{m\times n}(k))=mn$. 现在可以得出，若 B 为 k 上的一个 $n\times n$ 矩阵，则表 I，B，B^2，…，B^{n^2} 是线性相关的，因此存在不全为零的纯量 a_0，a_1，…，a_n^2 使得

$$a_0I+a_1B+\cdots+a_{n^2}B^{n^2}=0.$$

所以存在次数 $\leqslant n^2$ 的多项式 $f(x)\in k[x]$ 使得 $f(B)=0$. 这是凯莱-哈密顿(Cayley-Hamilton)定理一个“最弱的版本”，凯莱-哈密顿定理说，存在一个次数为 n 的多项式(特征多项式) $h_B(x)\in k[x]$

使得 $h_B(B)=0$.

推论 4.24 设 V 为一个向量空间且 $\dim(V)=n$.

(i)能张成 V 的含有 n 个向量的表一定是线性无关的.

(ii)任一个含有 n 个向量的线性无关的表一定可张成 V.

证明 (i)若 X 是线性相关的，则它可以缩短为 V 的一组基，而此基的元素个数又太少了.

(ii)若 Y 不能生成 V，则它可加长为 V 的一组基，而此基的元素个数又太多了. ■

→ **推论 4.25** 设 U 是维数为 n 的向量空间 V 的一个子空间. 则

(i)U 是有限维的.

(ii)$\dim(U)\leqslant\dim(V)$.

(iii)若 $\dim(U)=\dim(V)$，则 $U=V$. 336

证明 (i)取 $u_1\in U$. 若 $U=\langle u_1\rangle$，则 U 是有限维的. 否则，存在 $u_2\notin\langle u_1\rangle$. 由引理 4.21，$u_1$，$u_2$ 为线性无关的. 若 $U=\langle u_1, u_2\rangle$，则我们证毕. 此过程不能重复 $n+1$ 次，因为那样的话，u_1，…，u_{n+1}将会是 $U\subseteq V$ 中的线性无关的表，与推论 4.23 矛盾.

(ii)U 的一组基是线性无关的，因此它可以扩充为 V 的一组基. 从而 $\dim(U)\leqslant\dim(V)$.

(iii)若 $\dim(U)=\dim(V)$，则 U 的一组基也是 V 的一组基(否则它可以扩充 V 的一组基，而此基的元素又太多了). ■

例 4.26 在第 3 章中，**n 阶射影平面**被定义为满足 $|X|=n^2+n+1$ 的一个集合 X 和 X 的一族称为直线的子集，每条直线有 $n+1$ 个点，使得每两个点决定唯一一条直线. 若 q 是一个素数方幂，则我们可以通过给$\mathbb{F}_q^2$在无穷远处添加一条直线构造一个 q 阶射影平面.

我们现在来给出射影平面的第二个构造. 设 k 是一个域，$W=k^3$. k^3 中通过原点的一条直线 L 由它的任何一个非零向量的所有纯量倍组成：若 $v=(a, b, c)\in L$ 且 $v\neq(0, 0, 0)$，则

$$L=\{rv=(ra,rb,rc):r\in k\}.$$

当然，若 v'是 L 中的另一个非零向量，则 $L=\{rv':r\in k\}$. 因此 v 和 v'都扩张成 L 当且仅当它们都为非零的且 $v'=tv$，对某非零 $t\in k$. 在 k^3 的所有非零向量构成的集合上定义一个关系：

$$v=(a,b,c)\sim v'=(a',b',c')\text{ 若存在 } t\in k \text{ 使得 } v'=tv.$$

注意 $t\neq0$ 以免 $tv=(0, 0, 0)$. 易证~是 $W-\{(0, 0, 0)\}$上的一个等价关系. 我们记 $v=(a, b, c)$所在的等价类为

$$[v]=[a,b,c].$$

一个等价类[V]称为一个**射影点**，所有射影点构成的集合称为 k 上的**射影平面**，记为$\mathbb{P}^2(k)$. 若 π 是k^3 中通过原点的一个平面，(也就是，若 π 是 k^3 的一个 2 维空间)，则我们定义**射影直线**[π]是由所有满足 $v\in\pi$ 的射影点[V]构成的. ◀

推论 4.27 设 k 是一个域.

(i)$\mathbb{P}^2(k)$中每两个不同的点[v]和[v']在唯一一条射影直线上；

(ii)$\mathbb{P}^2(k)$中两条不同的射影直线[π]和[π']相交于唯一一个射影点. 337

证明 (i)[v]和[v']是射影点就是说 v 和 v'是 k^3 中的非零向量. [v]$\neq$[v']就是说 $v\not\sim v'$；

也就是无纯量 $t\neq 0$ 使得 $v'=tv$，因此 v，v' 是一个线性无关的表，所以存在一个唯一的平面 $\pi=\langle v, v'\rangle$ 通过原点且包含 v 和 v'. 从而 $[\pi]$ 是一个包含 $[v]$ 和 $[v']$ 的射影直线. 这条射影直线是唯一的，因为若 $[v]$，$[v']\in[\pi']$，则 v，$v'\in\pi'$，故由推论 4.25(iii)，$\pi=\pi'$，所以 $[\pi]=[\pi']$.

(ii)考虑 k^3 中的 $[\pi]$ 和 $[\pi']$. 由练习题 4.19，

$$\dim(\pi+\pi')+\dim(\pi\cap\pi')=\dim(\pi)+\dim(\pi').$$

因为 $\pi\neq\pi'$，我们有 $\pi\subsetneq\pi+\pi'$. 因此 $2=\dim(\pi)<\dim(\pi+\pi')\leqslant 3=\dim(k^3)$，从而 $\dim(\pi+\pi')=3$. 因此 $\dim(\pi\cap\pi')=2+2-3=1$，故 $[\pi\cap\pi']=[\pi]\cap[\pi']$ 是一个射影点. 交点是唯一的，否则与(i)相违. ■

命题 4.28 *若 $q=p^n$，p 为一个素数，则存在一个 q 阶射影平面.*

证明 设 $X=\mathbb{P}^2(k)$，其中 $k=\mathbb{F}_q$. 此时 $|k^3|=q^3$，故 k^3 中存在 q^3-1 个非零向量. 若 $v\in k^3$ 是非零的，则 $|[v]|=q-1$，因为 k 中存在 $q-1$ 个非零纯量. 因此 $|X|=(q^3-1)/(q-1)=q^2+q+1$. 最后，$k^3$ 中通过原点的平面 π 有 q^2-1 个非零向量，故 $|[\pi]|=(q^2-1)/(q-1)=q+1$. 由推论 4.27，$X$ 是一个 q 阶射影平面. ■

下面是射影平面的通常的定义.

定义 设 X 是一个集合，$\mathcal{L}$ 是 X 的一族子集，子集称为**直线**. 称 $(X, \mathcal{L})$ 为一个**射影平面**，若

(i)每两条直线相交于唯一一个点.

(ii)每两个点决定唯一一条直线.

(iii)X 中存在任三个点都不共线的 4 个点.

(iv)$\mathcal{L}$ 中存在任三条直线都不相交于同一个点的 4 条直线.

当 X 是有限这一特殊情形时，此定义与第 3 章中给出的定义是等价的.

定义关于 $(X, \mathcal{L})$ 的一个陈述的**对偶形式**为通过下面方式得到陈述：将点和线互换且将术语包含和包含于互换. 我们得出结论，关于射影平面任一个定理都可以产生一个**对偶定理**，它
338 的证明可通过在原来的证明中对每一个陈述对偶化而得到.

通过将 $\mathbb{P}^2(k)$ 的构造与第 3 章中 $k^2\cup\omega$ 的构造作比较，人们也可以看到对偶性，其中

$$\omega=\{\omega_\ell : \ell\text{ 是通过原点的一条直线}\}$$

是无穷远处的直线. 更详细地，设 $\ell=\{r(a, b) : r\in k\}$ 为 k^2 中通过原点的一条直线，其中 $(a, b)\neq(0, 0)$. 我们可记 ℓ 为 $[a, b]$ 且

$$\omega_\ell=\omega_{[a,b]}.$$

注意此记号与 $[a, b, c]\in\mathbb{P}^2(k)$ 是一致的；也就是，若 $\ell=\{r(a', b') : r\in k\}$，则存在一个非零的 $t\in k$ 使得 $(a', b')=t(a, b)$. 定义函数 $\varphi:\mathbb{P}^2(k)\to k^2\cup\omega$ 为

$$\varphi([a,b,c])=\begin{cases}(ac^{-1},bc^{-1}), & \text{若 } c\neq 0;\\ \omega_{[a,b]}, & \text{若 } c=0.\end{cases}$$

直接可以验证 φ 是一个(定义良好的)双射.

下引理的证明并不是困难的.

引理 一个子集 $\pi\subseteq k^3$ 是通过原点的一个平面当且仅当存在不全为零的 p，q，$r\in k$，满足 $\pi=\{(a, b, c)\in k^3 : pa+qb+rc=0\}$. 更进一步，若 $\pi'=\{(a, b, c)\in k^3 : p'a+q'b+r'c=$

0}，则 $\pi=\pi'$ 当且仅当存在一个非零的 $t\in k$ 满足 $(p', q', r')=t(p, q, r)$.

射影点几乎都有坐标：若 $v=(a, b, c)$，则我们称 $[a, b, c]$ 为射影点 $[v]$ 的**齐次坐标**(允许相差非零纯量倍数). 应用前一个引理，射影直线也几乎都有坐标：若 $\pi=\{(a, b, c)\in k^3: pa+qb+rc=0\}$，则我们称 $[p, q, r]$ 为射影直线 $[\pi]$ 的**齐次坐标**(允许相差纯量倍数). 双射 $\varphi: \mathrm{P}^2(k)\to k^2\cup\omega$ 保持直线不变，且射影平面中的对偶性可视为：用具有齐次坐标 $[a, b, c]$ 的射影点去替换具有相同齐次坐标的射影直线. ◀

现在我们可以将线性代数应用于域的研究中.

→ **命题 4.29(＝命题 3.119)** 若 E 为一个有限域，则 $|E|=p^n$，对某素数 p 及某 $n\geq 1$.

证明 由命题 3.110，E 的素域同构于 $\mathbb{F}_p$，对某素数 p. 因为 E 是有限的，它是有限维的，如设 $\dim E=n$. 若 $v_1, \cdots, v_n$ 是一组基，则的确存在 p^n 个向量 $a_1v_1+\cdots+a_nv_n\in E$，其中 $a_i\in\mathbb{F}_p$，对所有的 i. ■ 339

→ **定义** 若 k 为域 K 的一个子域，则我们通常说 K 为 k 的一个**扩张**，我们简记为"K/k 是一个扩张"⊖.

若 K/k 是一个扩张，则同例 4.1(iii)中一样，K 可以看成 k 上的一个向量空间. 称 K 为 k 的一个**有限扩张**若 K 是 k 上的一个有限维向量空间，K 的维数，记为 $[K:k]$，称为 K/k 的**次数**.

下面是称 $[K:k]$ 为次数的原因.

→ **命题 4.30** 设 E/k 为一个扩张，$z\in E$ 为一个不可约多项式 $p(x)\in k[x]$ 的一个根，且设 $k(z)$ 是 E 的包含 k 和 z 的最小子域. 则

$$[k(z):k]=\dim_k(k(z))=\deg(p).$$

证明 命题 3.116(iv)是说 $k(z)$ 中的每个元素有唯一的如下形式的表示 $b_0+b_1z+\cdots+b_{n-1}z^{n-1}$，其中 $b_i\in k$ 和 $n=\deg(p)$. 由命题 4.15，表 $1, z, z^2, \cdots, z^{n-1}$ 是 $k(z)$ 的一组基. ■

下面的公式是相当有用的，特别是在对次数用归纳法来证明某些定理时.

→ **定理 4.31** 设 $k\subseteq K\subseteq E$ 为域，K 为 k 上的有限扩张，E 是 K 上的有限扩张. 则 E 为 k 上的有限扩张，且

$$[E:k]=[E:K][K:k].$$

证明 设 $A=a_1, \cdots, a_n$ 是 K 在 k 上的一个基，$B=b_1, \cdots, b_m$ 是 E 在 K 的一个基，只须证明所有 a_ib_j 构成的表 X 是 E 在 k 上的一个基即可.

为证 X 生成 E，取 $e\in E$. 因为 B 为 E 在 K 上的一个基，所以存在纯量 $\lambda_j\in K$，使得 $e=\sum_j\lambda_jb_j$. 因为 A 是 K 在 k 上的一个基，所以存在纯量 $\mu_{ji}\in k$ 使得 $\lambda_j=\sum_i\mu_{ji}a_i$. 因此 $e=\sum_{ij}\mu_{ji}a_ib_j$，所以 X 在 k 上生成 E.

为证 X 在 k 上是线性无关的，我们假设存在纯量 $\mu_{ji}\in k$，使得 $\sum_{ij}\mu_{ji}a_ib_j=0$. 如果我们

⊖ 人们将 K/k 读成"K 在 k 之上". 不要将此记号与商环的记号混淆，因为 K 是一个域，因此它没有非零理想.

定义 $\lambda_j=\sum_i \mu_{ji}a_i$，则 $\lambda_j \in K$ 且 $\sum_j \lambda_j b_j=0$. 因为 B 在 K 上是线性无关的，所以对所有的 j，有

$$0=\lambda_j=\sum_i \mu_{ji}a_i.$$

340 因为 A 在 k 上是线性无关，从而对所有的 j 和 i，得出 $\mu_{ji}=0$，得证. ■

→ **定义** 设 E/k 为一个扩张且 $z\in K$. 我们称 z 为 k 上的**代数元**若存在以 z 为根的非零多项式 $f(x)\in k[x]$，否则称 z 为 k 上的**超越元**.

当我们说一个实数是一个超越数时，通常指的是它为Q 上的超越元. 例如，林德曼(F. Lindemann，1852—1939)在 1882 年证明了 π 是一个超越数，因此[Q (π) : Q]是无限维的(参见贝克(A. Baker)的《Transcendental Number Theory》第 5 页). 应用这个事实，我们可以看到，R 作为Q 上的向量空间是无限维的.（对于 π 的非有理性及更进一步的结果的证明，我们建议读者阅读尼温(Niven)和朱可曼(Zuckerman)的《An introduction to the Theory of Numbers》).

→ **命题 4.32** 若 K/k 是一个有限扩张，则每一个 $z\in K$ 是 k 上的代数元.

证明 若$[K:k]=n$，表 1，z，z^2，…，z^n 的长度为 $n+1$. 由推论 4.23，存在不全为零的 $a_i\in k$，使得 $\sum_{i=0}^{n} a_i z^i=0$. 若我们定义 $f(x)=\sum_{i=0}^{n} a_i x^i$，则 $f(x)$ 是一个非零多项式且 $f(z)=0$. 因此 z 是 k 上的代数元. ■

习题

H 4.1 判断对错，并说明理由.

(i)若 k 是一个域，则所有奇次数多项式构成的子集 E 是 $k[x]$的子空间.

(ii)设 A 和 B 是域 k 上的 $n\times n$ 矩阵且齐次方程组 $Ax=0$ 有非平凡的解，则齐次方程组$(BA)x=0$ 有非平凡的解.

(iii)设 A 和 B 是域 k 上的 $n\times n$ 矩阵且齐次方程组 $Ax=0$ 有非平凡的解，则齐次方程组$(AB)x=0$ 有非平凡的解.

(iv)若 v_1，v_2，v_3，v_4 生成 V，则 $\dim(V)=4$.

(v)若 k 是一个域，则表 1，x，x^2，…，x^{100} 在 $k[x]$中是线性无关的.

(vi)在 Mat_2(R)中，存在含 4 个矩阵的线性无关的表.

(vii)在 Mat_2(R)中，存在含 5 个矩阵的线性无关的表.

(viii)[Q $(E^{2\pi i/5})$: Q]=5.

(ix)在$\mathbb{R}^2$ 中，存在一个内积满足$(v, v)=0$，对某非零 $v\in \mathbb{R}^2$.

(x)所有满足 $f(1)=0$ 的 f : R →R 构成的集合是$\mathcal{F}$(R)的一个子空间.

*4.2 (i)设 k 为域，$f: k\to k$ 为一个函数. 设 $a\in k$，定义一个新的函数 $af: k\to k$ 为：$a\mapsto af(a)$. 证明在这种纯量乘法定义下，k 上所有的函数构成的环$\mathcal{F}(k)$是 k 上的一个向量空间.

341 (ii)用$\mathcal{PF}(k)\subseteq\mathcal{F}(k)$表示多项式函数 $a\mapsto \alpha_n a^n+\cdots+\alpha_1 a+\alpha_0$ 的全体. 证明$\mathcal{PF}(k)$是$\mathcal{F}(k)$的一个子空间.

4.3 证明 $\dim(V)\leqslant 1$ 当且仅当向量空间 V 的子空间只有{0}及 V 本身.

H 4.4 证明，在向量空间的定义中若其他公理都存在的话，则向量加法的交换律是多余的，也就是，若 V 满足所有其他公理，则对所有 u，$v\in V$，$u+v=v+u$.

4.5 若 L 是由所有 $n\times n$ 拉丁方构成的子集，那么 L 是 $\mathrm{Mat}_n(k)$的子空间吗？

4.6 (i)若 V 是$\mathbb{F}_2$ 上的一个向量空间且 $v_1 \neq v_2$ 是 V 中的非零向量. 试证 v_1, v_2 是线性无关的. 对于其他域上的向量空间，此结论成立吗?

(ii)设 k 为一个域，$P_2(k)$为由所有点$[x]$构成的射影平面，$x \in k^3$(与例 4.26 中一样). 试证在 $P_2(k)$中，$[x] \neq [y]$当且仅当 x, y 是 k^3 中的线性无关的表.

4.7 试证域 k 上的一个 $m \times n$ 矩阵 A 的列向量在 k^m 中是线性无关的当且仅当齐次方程组 $Ax=0$ 有非平凡解.

*4.8 **H** (i)试证多项式表 1, x, x^2, …, x^{100} 是 $k[x]$中的线性无关的表.

(ii)定义 $V_n = \langle 1, x, x^2, \cdots, x^n \rangle$. 试证 1, x, x^2, …, x^n 是 V_n 的一组基且得出结论 $\dim(V_n) = n+1$.

H 4.9 在解析几何中，我们证明了若 ℓ_1, ℓ_2 为两条非垂直的直线，斜率分别为 m_1 和 m_2，则 ℓ_1 与 ℓ_2 正交当且仅当 $m_1 m_2 = -1$. 若

$$\ell_i = \{\alpha v_i + u_i : \alpha \in \mathbb{R}\},$$

这里 $i=1, 2$，试证 $m_1 m_2 = -1$ 当且仅当点积 $v_1 \cdot v_2 = 0$.

4.10 (i)空间中通过点 u 的直线定义为

$$\{u + \alpha w : \alpha \in \mathbb{R}\} \subseteq \mathbb{R}^3,$$

这里 w 为一个固定的非零向量. 试证每一条通过点 u 的直线是$\mathbb{R}^3$ 的一个一维子空间的一个陪集.

H (ii)空间中通过点 u 的平面定义为

$$\{v \in \mathbb{R}^3 : (v-u) \cdot n = 0\} \subseteq \mathbb{R}^3,$$

这里 $n \neq 0$ 为一个固定的法向量且$(v-u) \cdot n$ 是一个点积. 试证通过点 u 的平面是$\mathbb{R}^3$ 的一个二维子空间的陪集.

*4.11 (i)证明 $\dim(\mathrm{Mat}_{m \times n}(k)) = mn$.

(ii)确定 $\dim(S)$，其中 S 是 $\mathrm{Mat}_n(k)$由所有对称矩阵构成的子空间.

4.12 设 $A \in \mathrm{Mat}_n(k)$，若 k 的特征不是 2，则 A 称为**斜对称的**若 $A^T = -A$，其中 A^T 为 A 的转置. 在 k 的特征为 2 时，A 称为**斜对称的**，若它是对称的且它的对角线上的元素全是 0.

(i)证明 $\mathrm{Mat}_n(k)$的由所有斜对称矩阵构成的子集 K 是 $\mathrm{Mat}_n(k)$的一个子空间.

(ii)确定 $\dim(K)$.

H 4.13 若 p 是一个素数且 $p \equiv 1 \bmod 4$，证明存在非零向量 $v \in \mathbb{F}_p^2$满足$(v, v)=0$，其中(v, v)是 v 与自己在通常意义下的内积(见例 4.4(i)). [342]

***H** 4.14 设 k 是一个域，且 k^n 具有通常意义下的内积. 试证若 $v = a_1 e_1 + \cdots + a_n e_n$，则 $a_i = (v, e_i)$，对所有的 i.

***H** 4.15 若 $f(x) = c_0 + c_1 x + \cdots + c_m x^m \in k[x]$，$A \in \mathrm{Mat}_n(k)$，定义

$$f(A) = c_0 I + c_1 A + \cdots + c_m A^m \in \mathrm{Mat}_n(k).$$

试证存在某非零 $f(x) \in k[x]$满足 $f(A)=0$.

*4.16 设 U 是域 k 上向量空间 V 的一个子空间，则 U 是 V 的一个子群(V 被视为一个加法交换群). 在商群 V/U 的陪集上定义纯量乘法如下:

$$\alpha(v+U) = \alpha v + U,$$

其中 $\alpha \in k$, $v \in V$. 证明这是一个定义良好的函数且使得 V/U 成为域 k 上的一个向量空间(V/U 称为一个**商空间**).

***H** 4.17 设 V 是一个有限维向量空间，U 是 V 的一个子空间. 试证

$$\dim(U) + \dim(V/U) = \dim(V).$$

由此得出结论 $\dim(V/U) = \dim(V) - \dim(U)$.

*4.18 设 $Ax=b$ 是一个线性方程组，s 是一组解. 若 U 是齐次线性方程组 $Ax=0$ 的解空间，试证 $Ax=b$ 的每

一个解都可以唯一地表示成如下形式 $s+u$，$u\in U$. 由此得出结论 $Ax=b$ 的解集是陪集 $s+U$.

*4.19 若 U 和 W 是向量空间 V 的子空间，定义

$$U+W=\{u+w: u\in U, w\in W.\}$$

(i)试证 $U+W$ 为 V 的一个子空间.

H(ii)设 U 和 U' 为有限维向量空间 V 的子空间. 试证

$$\dim(U)+\dim(U')=\dim(U\cap U')+\dim(U+U').$$

(iii)称子空间 $U\subseteq V$ 有补 S 若 $S\subseteq V$ 是子空间且 $U+S=V$ 和 $U\cap S=\{0\}$. 称 U 是 V 的直和项若 S 有补. 若 V 是有限维的，试证 V 的每个子空间 U 都是 V 的一个直和项(此结论在无限维向量空间中也成立，但证明要用佐恩(Zorn)引理).

*4.20 若 U 和 W 为域 k 上的向量空间，定义它们的直和为所有有序对构成的集合 $U\oplus W=\{(u, w): u\in U, w\in W\}$. 且加法为 $(u, w)+(u', w')=(u+u', w+w')$，纯量乘法为 $\alpha(u, w)=(\alpha u, \alpha w)$.

(i)试证 $U\oplus W$ 是一个向量空间.

(ii)若 U 和 W 是域 k 上的有限维向量空间，试证

$$\dim(U\oplus W)=\dim(U)+\dim(W).$$

*4.21 假设 V 为域 k 上的 $n-1$ 维向量空间且 V 有一个非退化的内积. 若 W 是 V 的一个 r 维子空间，试证

343 $V=W\oplus W^{\perp}$(见例 4.5). 由此得出结论 $\dim(W^{\perp})=n-r$.

4.22 下面是在 k^2 中成立的帕普斯(Pappus)定理，其中 k 是一个域. 设 ℓ 和 m 是不同的直线，A_1，A_2 和 A_3 是 ℓ 上的不同的点，B_1，B_2，B_3 是 m 上的不同的点. 定义 C_1 为 $A_2B_3\cap A_3B_2$，C_2 为 $A_1B_3\cap A_3B_1$ 且 C_3 为 $A_1B_2\cap A_2B_1$，则 C_1，C_2，C_3 是共线的.

陈述帕普斯定理的对偶定理(对偶在第 4.1 节中有定义).

→高斯消元法

下面这个域 k 上的奇次线性方程组可立即解出：

$$\begin{aligned}
x_1+\quad &+u_{1,m+1}x_{m+1}+\cdots+u_{1n}x_n=0\\
x_2+\quad &+u_{2,m+1}x_{m+1}+\cdots+u_{2n}x_n=0\\
&\vdots\\
x_m &+u_{m,m+1}x_{m+1}+\cdots+u_{mn}x_n=0.
\end{aligned}$$

替换 x_{m+1}，…，x_n 为常数 c_{m+1}，…，$c_n\in k$，我们有

$$x_i=-(u_{im+1}c_{m+1}+\cdots+u_{in}c_n),\text{对所有的 } i\leqslant m,$$

故任一个解具有形式

$$\left(-\sum_{j=m+1}^{n}u_{1j}c_j,\cdots,-\sum_{j=m+1}^{n}u_{mj}c_j,c_{m+1},\cdots,c_n\right).$$

此方程组的系数矩阵，

$$U=\begin{bmatrix}1&0&\cdots&0&u_{1,m+1}&\cdots&u_{1n}\\0&1&\cdots&0&u_{2,m+1}&\cdots&u_{2n}\\&\vdots&&\vdots&&\vdots&\\0&0&\cdots&1&u_{m,m+1}&\cdots&u_{mn}\end{bmatrix},$$

是一个阶梯形矩阵.

→ **定义** 一个 $m\times n$ 的矩阵 U 称为具有**行简化阶梯形**[⊖]若

(i)每一个所有元为零的行，如果有的话，位于每一个非零行的下方；

(ii)每一个非零行的**首元**(它的第一个非零的元)为 1；

(iii)每一个**首列**(包含一个首元的列)的其他元素为 0； 344

(iv)首列为 $\mathrm{COL}(t_1)$，…，$\mathrm{COL}(t_r)$，其中 $t_1<t_2<\cdots<t_r$ 且 $r\leqslant m$.

我们称 U **具有阶梯形**若它的首列是 COL(1)，COL(2)，…，COL(r)，也就是 $t_i=i$，对所有 $i\leqslant r$.

考虑矩阵

$$A=\begin{bmatrix}1&2&3&0&0\\0&0&0&1&5\\0&0&0&0&0\end{bmatrix}\quad 和\quad B=\begin{bmatrix}1&0&2&3&0\\0&1&0&0&5\\0&0&0&0&0\end{bmatrix}.$$

A 和 B 都是行简化阶梯形，但只有 B 是阶梯形.

定义 存在三种**初等行变换** $A\xrightarrow{o}A'$，将矩阵 A 变为矩阵 A'：

类型Ⅰ：o 将 A 的某一行的纯量倍加至另一行；也就是，o 替换 ROW(i)为 ROW(i)+cROW(j)，其中 $c\in k$ 是非零的，且 $j\neq i$；

类型Ⅱ：o 将非零 $c\in k$ 乘以 A 的某一行；也就是，o 替换 ROW(i)为 cROW(i)，其中 $c\in k$ 且 $c\neq 0$.

类型Ⅲ：o 将 A 的两行对换.

对一个矩阵，存在类似的**初等列变换**.

对换(类型Ⅲ)可由类型Ⅰ和类型Ⅱ的变换来实现(尽管它是多余的，但对换仍然被看成一个初等变换，因为它经常出现). 我们简单证明如下：

$$\begin{bmatrix}a&b\\c&d\end{bmatrix}\to\begin{bmatrix}a-c&b-d\\c&d\end{bmatrix}\to\begin{bmatrix}a-c&b-d\\a&b\end{bmatrix}\to\begin{bmatrix}-c&-d\\a&b\end{bmatrix}\to\begin{bmatrix}c&d\\a&b\end{bmatrix}.$$

回忆 ROW(A)，域 k 上矩阵 A 的行空间，是由 A 的行扩张的 k^n 的子空间；列空间，COL(A)，是 A 的列扩张的 k^m 的子空间.

→ **命题 4.33** 若 $A\to A'$ 是一个初等行变换，则 A 和 A' 具有相同的行空间：ROW(A)=ROW(A').

证明 假设 $A\to A'$ 是一个类型Ⅰ的初等变换. 则 A 的行空间是 $\mathrm{ROW}(A)=\langle\alpha_1,\cdots,\alpha_m\rangle$，其中 α_i 是 A 的第 i 行. 行空间 ROW(A′)是由 $\alpha_i+c\alpha_j$ 和 α_1，…，$\hat{\alpha}_i$，…，α_m 扩张而成的，其中 $c\in k$，$j\neq i$. 显然 $\mathrm{ROW}(A')\subseteq\mathrm{ROW}(A)$. 为证反包含，应注意到 $\alpha_i=(\alpha_i+c\alpha_j)-c\alpha_j\in\mathrm{ROW}(A')$. 345

若 $A\to A'$ 是一个类型Ⅱ的初等变换，则 ROW(A')是由 $c\alpha_i$ 和和 α_1，…，$\hat{\alpha}_i$，…，α_m 生成的，其中 $c\neq 0$. 显然 $\mathrm{ROW}(A')\subseteq\mathrm{ROW}(A)$. 为证反包含，应注意到 $\alpha_i=c^{-1}(c\alpha_i)\in\mathrm{ROW}(A')$.

不必考虑类型Ⅲ的初等变换，因为我们看到，这种类型的变换可以由一系列的其他两种类型的初等变换得到. ■

⊖ 原词为"*echelon*"，意为"翼"，因为首元的交错状况好像是鸟的翅膀.

→ **定义** 若 A 是域 k 上一个 $m\times n$ 的矩阵，其行空间为 $\mathrm{ROW}(A)$，则

$$\mathrm{rank}(A)=\dim(\mathrm{ROW}(A)).$$

→ **推论 4.34** 若 $A\to A'$ 是一个初等行变换，则

$$\mathrm{rank}(A)=\mathrm{rank}(A').$$

证明 更进一步的也成立，A 的行空间和 A' 的行空间是相等的，因此它们一定有相同的维数. ■

注 若 $A\to A'$ 是一个初等行变换，则 A 和 A' 可能会有不相同的列空间. 例如，考虑 $\begin{bmatrix}1&0\\1&0\end{bmatrix}\to\begin{bmatrix}1&0\\0&0\end{bmatrix}$. 然而一个矩阵的行空间和列空间具有相同的维数(见推论 4.84(ii)).

我们来证明若 $A\to A'$ 是一个初等行变换，则齐次方程组 $Ax=0$ 和 $A'x=0$ 有相同的解空间. 为此，我们引入**初等矩阵**的概念.

→ **定义** 设 o 为一个初等行变换，故 A' 可记为 $A'=o(A)$. 一个**初等矩阵**就是一个形如 $E=o(I)$ 的 $m\times m$ 的矩阵 E，其中 I 是 $m\times m$ 的单位矩阵. 若 o 是类型Ⅰ，Ⅱ，Ⅲ的初等变换，则我们说 $o(I)$ 是**类型Ⅰ，Ⅱ，Ⅲ的初等矩阵**.

下面是所有 2×2 的初等矩阵，其中 c 是一个非零纯量，

$$\begin{bmatrix}1&0\\c&1\end{bmatrix},\begin{bmatrix}1&c\\0&1\end{bmatrix},\begin{bmatrix}c&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&c\end{bmatrix},\begin{bmatrix}0&1\\1&0\end{bmatrix}.$$

对单位矩阵应用初等列变换产生同样的初等矩阵族.

下一个引理表明对矩阵 A 实施一次初等行变换的结果与对 A 左乘一个初等矩阵的结果是
346 一样的，而对实施一次初等列变换的效果与对 A 右乘一个初等矩阵的结果是一样的.

→ **引理 4.35** 若 A 是一个 $m\times n$ 矩阵且 $A\xrightarrow{o}A'$ 是一个初等行变换，则 $o(A)=o(\mathrm{I})A$；若 $A\xrightarrow{o}A'$ 是一个初等列变换，则 $o(A)=Ao(\mathrm{I})$.

证明 我们将仅仅解释结果，而将证明留给读者.

Type Ⅰ $$\begin{bmatrix}1&0&0\\0&1&0\\u&0&1\end{bmatrix}\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}=\begin{bmatrix}a&b&c\\d&e&f\\ua+g&ub+h&uc+i\end{bmatrix};$$

Type Ⅱ $$\begin{bmatrix}1&0&0\\0&u&0\\0&0&1\end{bmatrix}\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}=\begin{bmatrix}a&b&c\\ud&ue&uf\\g&h&i\end{bmatrix}.$$

同以前一样，此结论对类型Ⅲ的初等行变换也成立.

我们来解释一个初等列变换.

Type Ⅰ $$\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\u&0&1\end{bmatrix}=\begin{bmatrix}a+cu&b&c\\d+df&e&f\\g+iu&h&i\end{bmatrix}.$$ ■

回忆，一个 $n\times n$ 矩阵 A 是**非退化的**若存在一个 $n\times n$ 矩阵 B 使得 $AB=I$ 且 $BA=I$. 人们称 B 为 A 的逆，记之为 A^{-1}.

→ **命题 4.36** 每一个初等矩阵 E 都是一个非退化矩阵. 事实上，E^{-1}是一个与 E 同类型的初等矩阵.

证明 如果 o 是一个类型Ⅰ的初等行变换，则 o 替换 ROW(i)为 ROW(i)+cROW(j). 定义 o'为替换 ROW(i)为 ROW(i)−cROW(j)的初等行变换，我们断言初等矩阵 $E=o(I)$的逆就是 $o'(E)$. 引理 4.35 是说 $o(I)A=o(A)$，对每一个矩阵 A. 因此我们有：

$$E'E = o'(I)A = o'(E) = o'(o(I)) = I,$$

并且类似地，$EE'=I$. 注意到 E'是一个类型Ⅰ的初等矩阵.

若 o 是一个类型Ⅱ的初等行变换，则 o 替换 ROW(i)为 cROW(i). 定义 o'为替换 ROW(i)为 c^{-1}ROW(i)的初等行变换(这就是为什么我们要坚持假设 $c\neq 0$). 同前一段一样，若 $E'=o'(I)$，则 $E'E=I=E'E$. 注意到 E'是一个类型Ⅱ的初等矩阵.

类型Ⅲ的初等矩阵与它自己的逆相等：$EE=I$. ■

下面的引理是高斯消元法成立的关键. 347

引理 4.37 若 $A=A_0\to A_1\to\cdots\to A_p=B$ 是一系列的初等变换，则线性方程组 $Ax=0$ 和 $Bx=0$ 有相同的解空间.

证明 对 $p\geqslant 1$ 进行归纳. 设 S 和 S_1 分别是 $Ax=0$ 和 $A_1x=0$ 的解空间. 若 $A_1=o(A)$，则由引理 4.35，$A_1=EA$，其中 E 是初等矩阵 $o(I)$. 若 $v\in S$，则 $Av=0$；因此 $0=EAv=A_1v$，所以 $v\in S_1$. 反包含关系 $S_1\subseteq S$ 由等式 $A=E^{-1}A_1$ 可得，因为 E^{-1}也是一个初等矩阵. 归纳步的证明易得 ■

→ **推论 4.38** 若 A 和 B 是域 k 上的 $m\times n$ 矩阵，若存在一系列初等行变换

$$A = A_0 \to A_1 \to \cdots \to A_q = B,$$

则存在非退化矩阵 P 使得 $B=PA$. 若存在一序列初等列变换

$$B = B_0 \to B_1 \to \cdots \to B_r = C,$$

则存在非退化矩阵 Q 使得 $C=BQ$.

证明 对所有 $i\geqslant 1$，存在初等矩阵 E_i 使得 $A_i=E_iA_{i-1}$. 因此 $B=A_q=E_q\cdots E_2E_1A$. 定义 $P=E_q\cdots E_2E_1$，故 $B=PA$. 而 P 是非退化的，因为非退化矩阵的积还是非退化的[$(E_q\cdots E_2E_1)^{-1}=E_1^{-1}E_2^{-1}\cdots E_q^{-1}$]. 第二个论断类似可证. ■

回忆，若 $\sigma\in S_n$ 是一个置换，则一个 $n\times n$ 矩阵 Q_σ 称为是一个**置换矩阵**若它是由 σ 置换 $n\times n$单位矩阵的列而得的矩阵.

若 $\tau\in S_n$ 是一个轮换，则 Q_τ 是对换单位矩阵的两列而得到的，因此它是一个类型Ⅲ的初等矩阵(记住，对 I 实施一个初等列变换产生一个初等矩阵). 因为每一个置换 σ 是一些轮换的积(命题 2.35)，因此 Q_σ 是初等矩阵的积.

若 $Ax=0$ 是一个齐次方程组，则 A 的第 i 个列向量对应于第 i 个变量：COL(i)对应于 x_i. 对 A 的列用 σ 进行置换得到矩阵 AQ_σ，这样 AQ_σ 对应于"同样的"齐次方程组$(AQ_\sigma)y=0$，它的变量 $y_i=x_{\sigma(i)}$仅仅是对原来的变量再重新编号而已.

→ **定义** 称矩阵 A 是**高斯等价**于矩阵 B 的若存在一系列的初等行变换

$$A = A_0 \to A_1 \to \cdots \to A_p = B.$$ 348

易证高斯等价是所有 $m\times n$ 矩阵集合的一个等价关系．若 A 和 B 是高斯等价的矩阵，则由推论 4.34 可推出 A 和 B 有相同的秩，且引理 4.37 表明 $Ax=0$ 和 $Bx=0$ 有相同的解空间．

→ **定理 4.39(高斯消元法)** (i)域 k 上每一个 $m\times n$ 矩阵 A 都高斯等价于一个具有行简化阶梯形的矩阵 U．

(ii)在(i)中的矩阵 U 是由 A 唯一确定的．

(iii)存在非退化矩阵 P 和一个置换矩阵 Q_σ 使得 PAQ_σ 具有阶梯形．

证明 (i)对 n 进行归纳，n 为 A 的列数．

设 $n=1$．若 $A=0$，证明完成．若 $A\neq 0$，则对某个 j，$a_{j1}\neq 0$．用 a_{j1}^{-1} 乘 ROW(j)，并且对换 ROW(j)和 ROW(1)，这样新矩阵 $A'=[a'_{p1}]$中 $a'_{11}=1$．对每个 $p>1$，替换 a'_{p1} 为 $a'_{p1}-a'_{p1}a'_{11}=0$．我们已经得到一个 $m\times 1$ 行简化阶梯形矩阵，因为它的第一行元素为 1，而所有其他行的元素为 0．

为证明归纳步，设 A 为一个 $m\times(n+1)$矩阵．若 A 的第一列为 0，则由归纳，可将此矩阵的后 n 列构成的矩阵化为行简化阶梯形，结果 A 就化为行简化阶梯形了．若 A 的第一列不是 0，将它的第一列化为行简化阶梯形(在基础步骤中一样)，这样就得到新的矩阵 $A'=\begin{bmatrix}1 & Y\\ 0 & M\end{bmatrix}$，其中 M 是一个$(m-1)\times n$ 矩阵．读者的第一个猜想与在基础步骤中一样，对 A'的后 n 列构成的矩阵应用归纳假设．这是不方便的，因为初等行变换也许是将 ROW(1)的倍数加至另一行，从而改变了第一列．我们而是用归纳假设将 M 替换为 D，其中 D 是一个高斯等价于 M 的行简化阶梯形矩阵．因此 A'高斯等价于 $N=\begin{bmatrix}1 & Y\\ 0 & D\end{bmatrix}$．设(0，$D$)的首列是 COL($t_2$)，…，COL($t_r$)，其中 $2\leqslant t_2<\cdots<t_r$($D$ 的第一列为 N 的第 2 列)．也许元素 $y_{i,t_2}\neq 0$．如果是这样，替换 N 的 ROW(1)为 ROW(1)$-y_{i,t_1}$ROW(2)(D 的第一行为 N 的第二行)．因为 COL(t_2)的首元的左边的元素为 0，故此变换不改变 N 的在 COL(t_2)左边的列．因此，COL(t_2)中的首元就是此列中仅有的非零元素，而且 COL(1)不能改变．接下来，用同样的方式使得 $y_{1,t_3}\neq 0$(COL(1)和 COL(t_2)不被改变)，继续下去，直到所有的 $y_{1,t_i}=0$．我们就得到一个行简化阶梯形矩阵．其首列为 COL(1)，COL(t_2)，…，COL(t_r)．

(ii)假设 U 是一个高斯等价于 A 的行简化阶梯矩阵．设 U 的非零行为 β_1，…，β_r．设 U 的
349 首列为 COL(t_1)，COL(t_2)，…，COL(t_r)．设 $\beta_i=e_{t_i}+v_i$，其中 $v_i\in\langle e_v : v\rangle t_i$(与通常一样，$e_1$，…，$e_n$ 是 k^n 的标准基)．我们断言，COL(t_1)，COL(t_2)，…，COL(t_r)就是 U 的满足以下性质的列：$\langle\beta_1,\cdots,\beta_r\rangle=$ROW($U$)中非零向量的首元一定在这些列中．由此得出首列是由 ROW(U)确定的．显然 COL(t_i)包含一个首元(我们称为 β_i 的首元)．另一方面，若 γ 是$\langle\beta_1,\cdots,\beta_r\rangle$中的一个非零向量，则 $\gamma=c_1\beta_1+\cdots+c_r\beta_r$．若我们将 β_i 想象成 U 的第 i 行，则用 c_i 乘 ROW(i)，再相加：γ 就是这个和式，且它的第 j 个坐标就是第 j 列的元素和．因此对每个 i，γ 的第 t_i 个坐标就是 c_i，因为在 COL(t_i)中的没有其他的非零元素．因为 $\gamma\neq 0$，故存在某些 $c_i\neq 0$．我们断言第一个不为零的，如 $c_{t_{i_0}}$，是它的首元．现在当 $i<i_0$ 时，所有的 $c_i=0$，所以 $\gamma=c_{i_0}e_{i_0}+\omega$，其中 $\omega=\sum\limits_{i>i_0}c_iv_i\in\langle e_v : v>t_{i_0}\rangle$．因此 γ 的首元在 COL(t_{i_0})中．

若U'是另一个高斯等价于 A 的行简化阶梯形矩阵，则命题 4.33 是说 ROW(U')＝ROW(U)。因为我们刚刚证明了行空间确定首列，所以 U'和 U 的首列是一样的．设 U'的非零行为β_1'，…，β_r'．因为 $\beta_i'\in$ ROW(U)＝ROW(U')，所以存在 $c_v\in k$ 满足 $\beta_i'=\sum_v c_v\beta_v$．在前一段中我们看到，对每个 v，β_i'的第 t_v 个坐标为 c_v．因此 $c_i=1$，而其他的 $c_v=0$，所以对所有的 i 有 $\beta_i'=\beta_i$．从而 $U'=U$．

(iii)选择 σ 为满足对 $i=1$，…，r 有 $\sigma(t_i)=i$ 的任一个置换． ■

推论 4.40 设 A 为域 k 上的一个 $m\times n$ 矩阵．若 rank(A)＝m，则对每一个 $b\in k^m$（非奇次）线性方程组 $AX=b$ 是相容的．

证明 若 U 是一个秩为 m 的 $m\times n$ 阶梯形矩阵，则它没有零行．对任一个 $c\in k^m$，线性方程组 $Ux=c$ 为

$$\begin{aligned} x_1 + \quad\; &+u_{1,m+1}x_{m+1}+\cdots+u_{1n}x_n = c_1\\ x_2 + \quad &+u_{2,m+1}x_{m+1}+\cdots+u_{2n}x_n = c_2\\ &\quad\vdots \qquad\qquad\qquad \vdots \qquad\qquad\quad \vdots\\ x_m &+u_{m,m+1}x_{m+1}+\cdots+u_{mn}x_n = c_m. \end{aligned}$$

$x_i=c_i-(u_{i,m+1}d_{m+1}+\cdots+u_{in}d_n)$给出它的一个解，其中 d_{m+1}，…，$d_n\in k$．

由高斯消元法知，存在一个非退化矩阵 P 和一个置换矩阵 Q 满足 $PAQ=U$，U 为阶梯形．我们刚刚看到方程组 $Ux=PbQ$ 有一个解，故方程组 $P^{-1}UQ^{-1}x=P^{-1}(PbQ)Q^{-1}$，也就是，$Ax=b$ 有一个解． ■

→ **推论 4.41** 设 A 为域 k 上的一个 $m\times n$ 矩阵．若 U 是 A 的行简化阶梯形，则 ROW(A)的一组基可由 U 的非零行组成． 350

证明 由命题 4.33 知 ROW(A)＝ROW(U)．因此 ROW(U)由 U 的行扩张而成．显然 U 的非零行是线性无关的，所以它们构成 ROW(U)＝ROW(A)的一组基． ■

我们刚刚看到了如何求 rank(A)：将 A 化为阶梯形 U，则 rank(A)是 U 中非零行的行数．

→ **定义** 若 U 是一个 $m\times n$ 的行简化阶梯矩阵，其首列为 COL(t_1)，…，COL(t_r)．则 x_{t_1}，…，x_{t_r}称为**固定变量(或主要变量)**，而其余的变量称为**自由变量**．

回忆，高斯消元法解线性代数的方法是替换矩阵 A 为与它高斯等价的阶梯矩阵 U．例如，齐次线性方程组 $Ax=0$ 的解空间与 $Ux=0$ 的解空间是一样的．而 $Ux=0$ 是容易求解的，像前面的一样．下一个定理表明任一个齐次线性方程组的求解是不会比前面最简单的方程的求解更困难的．

定理 4.42 设 $Ax=0$ 为一个线性方程组，其中 A 是域 k 上一个 $m\times n$ 的矩阵．设 $U=[u_{ij}]$为高斯等价于 A 的(唯一的)阶梯形矩阵．必要时对变量重新标号，则 $Ax=0$ 的解空间 $Sol(A)$由所有具有下列形式的向量组成

$$\left(-\sum_{\ell=r+1}^{n}u_{1\ell}c_\ell,\cdots,-\sum_{\ell=r+1}^{n}u_{r\ell}c_\ell,c_{r+1},\cdots,c_n\right).$$

证明 由引理 4.37，n 元有序元素组 $s=(c_1$，…，$c_n)$是 $Ax=0$ 的一个解当且仅当它是 $Ux=0$的一个解．由定理 4.39，存在一个置换 σ 使得 UQ_σ 是阶梯形．注意置换列仅仅是对变

量重新标号，因此不失一般性. 假设 U 是阶梯形矩阵，也就是前 r 个变量是固定变量，后 $n-r$ 个变量是自由变量. 这样 U 具有形式

$$B=\begin{bmatrix}1 & 0 & \cdots & 0 & u_{1,r+1} & \cdots & u_{1n}\\ 0 & 1 & \cdots & 0 & u_{2,r+1} & \cdots & u_{2n}\\ & \vdots & & \vdots & & \vdots & \\ 0 & 0 & \cdots & 1 & u_{r,r+1} & \cdots & u_{rn}\\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0\\ & \vdots & & \vdots & & \vdots & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0\end{bmatrix},$$

351 因此像在定理 4.39 的证明中一样，结论成立. ■

→ **定理 4.43(秩-零化度定理)** 设 A 为域 k 上的一个 $m\times n$ 的矩阵. 若 $Sol(A)$ 为齐次线性方程组 $Ax=0$ 的解空间，则

$$\dim(Sol(A))=n-r,$$

其中 $r=\operatorname{rank}(A)$.

证明 我们不妨假设变量已经重新标号了，这样固定变量排在所有自由变量的前面. 对每一个满足 $1\leqslant\ell\leqslant n-r$ 的 ℓ，定义对所有的 $\upsilon\neq\ell$，s_ℓ 为满足 $c_{p_\ell}=1$ 和 $c_{p_\upsilon}=0$ 的解 $s_\ell=(c_1,\cdots,c_n)$. 因此

$$\begin{aligned}s_1&=(-u_{1,r+1},-u_{2,r+1},\cdots,-u_{r,r+1},1,0,\cdots,0)\\ s_2&=(-u_{1,r+2},-u_{2,r+2},\cdots,-u_{r,r+2},0,1,\cdots,0)\\ &\vdots\\ s_{n-r}&=(-u_{1,n},-u_{2,n},\cdots,-u_{r,n},0,0,\cdots,1)\end{aligned}$$

这 $n-r$ 个向量是线性无关的(注意它们的后 $n-r$ 个坐标). 而定理 4.42 表明它们扩张成 $Sol(A)$：

$$\left(-\sum_{\ell=r+1}^{n}u_{1\ell}c_\ell,\cdots,-\sum_{\ell=r+1}^{n}u_{r\ell}c_\ell,c_{r+1},\cdots,c_n\right)=\sum_{\ell=r+1}^{n}c_\ell s_\ell.$$ ■

方程组 $Ax=0$ 的解空间的维数 $n-r$ 经常被称为一般解的**自由度**.

例 4.44 考虑矩阵

$$A=\begin{bmatrix}0 & 0 & 1 & 1 & 0\\ -2 & -4 & 1 & 0 & -3\\ 3 & 6 & -1 & 1 & 5\end{bmatrix}.$$

求 $\operatorname{rank}(A)$以及它的行空间的一组基，并且求齐次方程组 $Ax=0$ 的解空间的一组基.

矩阵 A 高斯等价于

$$B=\begin{bmatrix}1 & 2 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 & -1\\ 0 & 0 & 0 & 1 & 1\end{bmatrix}.$$

因此 $\operatorname{rank}(A)=3$ 且行空间的一组基为(1, 2, 0, 0, 1), (0, 0, 1, 0, −1)和(0, 0, 0, 1, 1).

注意 A 的行向量是线性无关的，因为它扩张成一个 3 维空间(参阅推论 4.24). 固定变量是 x_1，x_3 和 x_4，而自由变量为 x_2 和 x_5，解空间的维数为 $5-3=2$. 方程组 $Bx=0$ 是 352

$$\begin{aligned} x_1+2x_2+x_5&=0\\ x_3-x_5&=0\\ x_4+x_5&=0 \end{aligned}$$

一般解为$(-2c-d,\ c,\ d,\ -d,\ d)$. ◀

习题

H 4.23 判断对错并说明理由.

(i)若 A 是一个三角形矩阵，则 $n\times n$ 的非齐次方程组 $Ax=b$ 有解.

(ii)高斯等价的矩阵具有相同的行空间.

(iii)高斯等价的矩阵具有相同的列空间.

(iv)矩阵 $A=\begin{bmatrix}1&0&0\\0&1&-1\\0&0&1\end{bmatrix}$ 是非退化的.

(v)域上每一个非退化的矩阵是初等矩阵的积.

(vi)若 A 是一个 $m\times n$ 矩阵，则 $\mathrm{ROW}(A^{\mathrm{T}})=\mathrm{COL}(A)$.

4.24 (i)试证向量空间 V 中的一个表 v_1，…，v_m 是线性无关的当且仅当它扩张成 V 的一个 m 维子空间.

H (ii)判断 k^4 中下表是否是线性无关的

$$v_1=(1,1,-1,2),v_2=(2,2,-3,1),v_3=(-1,-1,0,-5).$$

H 4.25 向量 $v_1=(1,\ 4,\ 3)$，$v_2=(-1,\ -2,\ 0)$和 $v_3=(2,\ 2,\ 3)$能扩张成 k^3 吗?

*4.26 (i)一个 $n\times n$ 的矩阵是**三角形矩阵**若它的所有在对角线下方的元素全为零或者所有在对角线上方的元素全为零. 试证明每一个 $n\times n$ 的行简化阶梯形矩阵是三角形矩阵.

(ii)应用定理 4.39 证明，每一个 $n\times n$ 的矩阵 A 均高斯等价于一个三角形矩阵.

H 4.27 设 k 是一个域，A 为 k 上的一个 $n\times m$ 的矩阵. 一个(非齐次)线性方程组 $Ax=\beta$，其中 $\beta\in k^n$，称为是**相容的**若存在 $v\in k^n$ 使得 $Av=\beta$. 证明，$Ax=\beta$ 是相容的当且仅当 β 在 A 的列空间中. (回忆习题 418：相容的非齐次线性方程组 $Ax=\beta$ 的解集是 $Ax=0$ 的解空间的一个陪集).

4.28 若 A 是一个 $n\times n$ 的非退化矩阵，试证任一个方程组 $Ax=b$ 有唯一的解，也就是 $x=A^{-1}b$.

4.29 设 α_1，…，α_n 为域 k 上一个 $m\times n$ 的矩阵 A 的列向量，并设 $\beta\in k^m$.

(i)试证 $\beta\in\langle\alpha_1,\ \cdots,\ \alpha_n\rangle$ 当且仅当非齐次线性方程组 $Ax=\beta$ 有解. 353

H (ii)定义**增扩矩阵**$[A\mid\beta]$为 $m\times(n+1)$的矩阵，它的开始的 n 列是 A，最后一列为 β. 试证 β 在 A 的列空间中当且仅当 $\mathrm{rank}([A\mid\beta])=\mathrm{rank}(A)$.

(iii)问 $\beta=(0,\ -3,\ 5)$在由 $\alpha_1=(0,\ -2,\ 3)$，$\alpha_2=(0,\ -4,\ 6)$，$\alpha_3=(1,\ 1,\ -1)$生成的子空间中吗?

4.30 (i)试证域 k 上的 $n\times n$ 矩阵 A 是非退化的当且仅当它高斯等价于单位矩阵 I.

H (ii)求下矩阵的逆矩阵

$$A=\begin{bmatrix}2&3&1\\-1&1&0\\1&0&1\end{bmatrix}.$$

*4.31 (i)设 $Ax=b$ 为域 k 上的一个 $m\times n$ 的线性方程组. 试证明它存在一个满足 $x_{j_1}=0=x_{j_2}=\cdots=x_{j_s}$ 的解 $x=(x_1,\ \cdots,\ x_n)$当且仅当 $m\times(n-s)$方程组 $A^*x^*=b$ 有解，其中 $s\leqslant n$，A^* 是从 A 中删掉第 j_1，

j_2，…，j_t 列后所得的矩阵.

H (ii)试证明若(i)中的矩阵 A^* 的秩为 m，则 $Ax=b$ 存在满足 $x_{j_1}=0=x_{j_2}=\cdots=x_{j_t}$ 的解.

4.2 欧氏作图

古代文明中的一些神话说到，上帝要求人类给出一些数学问题的准确答案，以作为从灾难中解救人类的报答. 我们引用范德瓦尔登(van der Waerden)的《古代文明中的几何与代数》(Geometry and Algebra in Ancient Civilizations)一书中的下面一段：

> 在埃拉托色尼(Eratosthenes)的对话"柏拉图式的"中，讲述了一个关于倍立方体的问题的故事. 士麦那[1]的塞翁(Theon)在他的名为《阅读柏拉图的所要用的数学知识的解释》一书中描述到，根据这个故事，得洛斯[2]人请求一个先贤将他们的从灾难中解救出来，上帝(阿波罗神)通过一个先贤回答到，他们必须建造一个外形不变的且大小为现有的 2 倍的新祭坛. 得洛斯人派一个代表团求教柏拉图，但柏拉图将他们引见给了基则克斯(Kyzikos)的数学家欧多克索斯(Eudoxos)和赫林肯(Helikon).

祭坛在外形上是立方体，所以此问题关系到如何作 $\sqrt[3]{2}$. 上帝是残酷的，因为尽管几何上有作 $\sqrt{2}$ 的方法(就是边长为 1 的正方形的对角线的长度)，但是我们将证明用欧氏几何的方法即仅用直尺与圆规是不可能作出 $\sqrt[3]{2}$ 来的. 实际上，上帝也没那么残酷，因为希腊人可用其他方法. 例如门奈赫莫斯(Menaechmus)就是用抛物线 $y^2=2x$ 和 $x^2=y$ 的交来作 $\sqrt[3]{2}$ 的. 这对我们来说是浅显的，但在没有解析几何和代数的时代，这的确是一个具有独创
354 精神的伟绩.

从希腊也流传下来一些其他的几何问题. 能不能三等分每一个角？能不能作出一个正 n 边形？能不能"化圆为方"，也就是能不能画个正方形使得它的面积等于给定圆的面积？

记号 设 P 和 Q 为平面上的两点，我们记端点为 P 和 Q 的线段为 PQ，我们记此线段的长度为 $|PQ|$. 用 $L[P, Q]$ 表示由 P，Q 确定的直线，用 $C[P; PQ]$ 表示圆心为 P 半经为 $|PQ|$ 的圆.

没有作图的准确的定义，这些经典问题可能显得非常简单. 例如，一个 60°角可以用量角器三等分：只要找到 20°，再画出此角即可. 因此把问题讲清楚和做一定的假设是必要的. 希腊问题强调只能用两种工具，且每一种只能有一种用法. 给定平面中不同的点 P 和 Q，**直尺**是一个能画出直线 $L[P, Q]$ 的工具. **圆规**是一个能分别画出圆心为 P 或 Q 半经为 $|PQ|=|QP|$ 的圆 $C[P; PQ)$ 和 $C[Q; QP]$ 的工具.

我们说的是直尺，也有的人称为**米尺**[3]. 我们用第一个术语以免产生混乱，因为米尺有额外的功能：人们可以在米尺上标记出两点，如 P 和 Q，且此标记的点 P 允许在一条曲线上滑动. 这个增加了米尺的证明功能使其成为了一个更有力的仪器. 大约在公元前 425 年，埃理斯(Elis)的希皮尔斯(Hippias)就能够用某些曲线、直线和圆化圆为方. 尼科米迪斯(Nicomedes)

[1] 士麦那(Smyrna)是土耳其的港口城市——译者注.

[2] 得洛斯(Delians)是爱琴海中的小岛——译者注.

[3] 在原书中，米尺(ruler)指带刻度的直尺，直尺(straightedge)指不带刻度的尺——译者注.

就是只用米尺与圆规解决了德理人的倍立方体问题．尼科米迪斯和阿基米德用这些工具也能三等分任意角．

一般来说，我们可以利用已有的点 P，Q，R 和 S(不必不同)按照下面的方式作出一个新点：用第一对点 P，Q 去画一条直线或一个圆，再用第二对点 R，S 去画一条直线或一个圆．这样就能得到已画出的两条直线或一条直线与一个圆或两个圆的交点 T．更一般地，一个点称为是可构作的点，若它可以从(1，0)与(0，−1)出发用有限步这样的步骤得到．给定一对可构作的点，我们并不能假定它们决定的直线或圆上的所有点都是可构作的．

当我们说解决经典问题是不可能的(仅用直尺和圆规)时候，我们知道说了什么，我们的意思不只是说这仅仅是很困难的．读者应思考我们是如何证明有一些东西是不可能的．

下面来进行正式的讨论．

给定一个平面，我们通过两个不同的点 A 和 $\overline{A}$ 来确定一个坐标系．称由 A 和 $\overline{A}$ 确定的直线为 **x-轴**．用圆规分别画出以 $|A\overline{A}|$ 为半经以 A 或 $\overline{A}$ 为圆心的两个圆 $C[A; A\overline{A}]$ 和 $C[\overline{A}; \overline{A}A]$．由这两个圆交出两点确定的直线称为 **y-轴**．它垂直等分 $A\overline{A}$，与 x-轴的交点 O 称为**原点**．我们规定长度 $|OA|$ 为 1．这样我们就在平面上建立了坐标系，特别地，$A=(1, 0)$ 355
和 $\overline{A}=(-1, 0)$．

定义 设 $E\neq F$ 且 $G\neq H$ 为平面上的点．点 Z 称为**从 E，F，G，H 出发可构作的**，若下列之一成立：

(i) $Z\in L[E, F]\cap L[G, H]$，其中 $L[E, F]\neq L[G, H]$；

(ii) $Z\in L[E, F]\cap C[G; GH]$，或 $Z\in L[G, H]\cap C[E; EF]$；

(iii) $Z\in C[E; EF]\cap C[G; GH]$，其中 $C[E; EF]\neq C[G; GH]$．

点 Z 称为**可构作的**若 $Z=A$ 或 $Z=\overline{A}$ 或存在点 P_1，…，P_n 使得点 $Z=P_n$，且对所有的 $j\geqslant 1$，点 P_{j+1} 是可从 $\{A, \overline{A}, P_1, \cdots, P_j\}$ 中的点出发可构作的．

例 4.45 下面证明点 $Z=(0, 1)$ 是可构作的．从图 4-1 可看出，点 $P_1=(0, \sqrt{3})$，$P_2=(0, -\sqrt{3})$ 是可构作的，因为它们都在 $C[A; A\overline{A}]\cap C[\overline{A}; \overline{A}A]$ 中．因此 y-轴 $L[P_1, P_2]$ 可以作出．最后

$$Z=(0,1)\in L[P_1,P_2]\cap C[O;OA]. \quad ◀$$

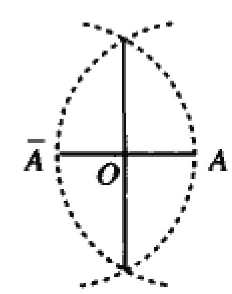


图 4-1 第一可构作的点

在下面的讨论中，我们将自由地使用欧氏空间中任意的标准结果．例如，每个角可用尺规二等分，即若 $(\cos\theta, \sin\theta)$ 是可构作的，则 $\left(\cos\frac{\theta}{2}, \sin\frac{\theta}{2}\right)$ 也是可构作的．

定义 复数 $z=x+iy$ 称为是**可构作的**，若点 (x, y) 是一个可构作的点．

例 4.45 表明数 1，−1，0，$i\sqrt{3}$，$-i\sqrt{3}$，i 及 −i 均为可构作的复数． 356

引理 4.46 复数 $z=x+iy$ 是可构作的当且仅当它的实部 x 与虚部 y 均是可构作的．

证明 若 z 是可构作的，则用一个标准的欧氏构作可画一条通过 (x, y) 的且平行于 y 轴的垂线．因为作为 L 和 x 轴的交点，$(x, 0)$ 是可构作的，从而 x 是可构作的．类似地，点 $(0, y)$ 是 y-轴与一条通过点 (x, y) 且平行于 x 轴的直线的交点．$P(y, 0)$ 也是可构作的，因为它

是 x-轴与 $C[O;\ OP]$的交点. 所以 y 为可构作的数.

反之，假设 x 与 y 是可构作的数，即 $Q=(x,\ 0)$和 $P=(y,\ 0)$是可构作的点. 作为 y 轴与 $C[O;\ OP]$的交点，点$(0,\ y)$是可构作的. 画出通过$(x,\ 0)$的垂线和通过$(0,\ y)$的水平线，则$(x,\ y)$为它们的交点，因此$(x,\ y)$是一个可构作的点，从而 $z=x+\mathrm{i}y$ 是一个可构作的数. ■

记号 用 K 表示$\mathbb{C}$ 中所有**可构作的数**组成的集合.

定理 4.47 所有可构作的实数组成的集合 $K\cap\mathbb{R}$ 是$\mathbb{R}$ 的一个它的正元素在平方根下封闭的子域.

证明 设 a，b 为可构作的实数.

(i)$-a$ 是可构作的. 若 $P(a,\ 0)$为可构作的点，则$(-a,\ 0)$是 x-轴与 $C[O;\ OP]$的另一个交点.

(ii)$a+b$ 和$-a+b$ 是可构作的. 如图 4-2 所示 .

假设 a，b 为正的. 令 $I=(0,\ 1)$，$P=(a,\ 0)$，$Q=(b,\ 1)$. Q 是可构作的：因为它是通过 I 的水平线与通过$(b,\ 0)$[由假设知此点是可构作的]的垂线的交点. 通过 Q 点且平行于 IP 的直线与 x-轴交于点 $S(a+b,\ 0)$，得证.

若我们替换 $P(a,\ 0)$为 $P'(-a,\ 0)$，同样的方法可构作$-a+b$，点$(-a+b,\ 0)$是 x-轴与

357 通过 $Q=(b,\ 0)$平行于 I 直线的交点.

(iii)ab 是可构作的.

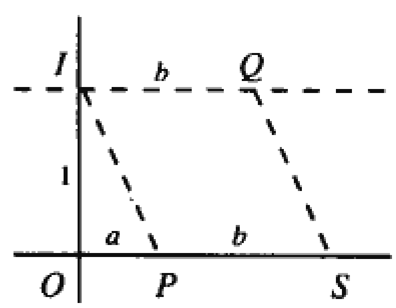


图 4-2 $a+b$

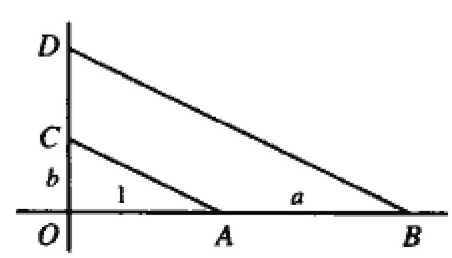


图 4-3 ab

由(i)，我们可以假定 a 和 b 都是正的. 在图 4-3 中，$A=(1,\ 0)$，$B=(1+a,\ 0)$，$C=(0,\ b)$. 定义 D 为 y-轴与通过 B 且平行于 AC 的直线的交点. 因为三角形$\triangle OAC$ 和$\triangle OBD$ 是相似的，所以

$$|OB|/|OA|=|OD|/|OC|;$$

因此$(a+1)/1=(b+|CD|)/b$，从而 $|CD|=ab$. 所以 $b+ab$ 是可构作的. 由(i)得$-b$ 是可构作的. 再由(ii)，就有 $ab=(b+ab)-b$ 是可构作的.

(iv)若 $a\neq 0$，则 a^{-1}是可构作的. 如图 4-4 所示 . 令 $A=(1,\ 0)$，$S=(0,\ a)$且 $T=(0,\ 1+a)$. 定义 B 为 x-轴与通过 T 且平行于 AS 的直线的交点，则对某个 u，$B=(1+u,\ 0)$，三角形$\triangle OSA$ 与$\triangle OTB$ 的相似性给出

$$|OT|/|OS|=|OB|/|OA|.$$

因此$(1+a)/a=(1+u)/1$，所以 $u=a^{-1}$. 从而 $1+a^{-1}$是可构作的，所以$(1+a^{-1})-1=a^{-1}$是可构作的.

(v)若 $a\geqslant 0$，则 $\sqrt{a}$ 是可构作的．如图 4-5 所示．设 $A=(1,0)$，$P=(1+a,0)$；作 OP 的中点 Q．定义 R 为圆 $C[Q;QO]$ 与通过 A 的垂线的交点．(右边的)三角形 $\triangle AOR$ 和 $\triangle ARP$ 是相似的，所以

$$|OA|/|AR|=|AR|/|AP|,$$

从而 $|AR|=\sqrt{a}$． ■ 358

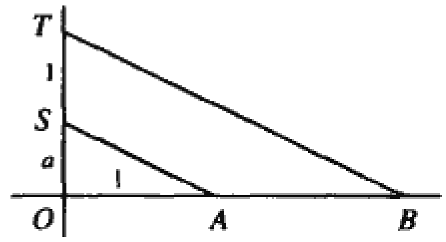


图 4-4 a^{-1}

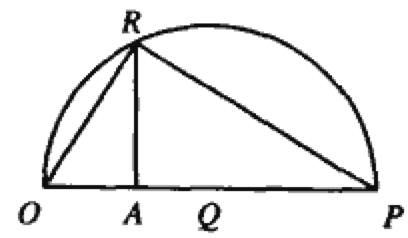


图 4-5 $\sqrt{a}$

推论 4.48 *所有可构作的数组成的集合 K 是 $\mathbb{C}$ 的一个在平方根下封闭的子域.*

证明 若 $z=a+ib$ 和 $w=c+id$ 为可构作的，那么由定理 4.47，a，b，c，d 是可构作的，所以 $a,b,c,d\in K\cap\mathbb{R}$．因为 $K\cap\mathbb{R}$ 是 $\mathbb{R}$ 的一个子域，故 $a\pm b$，$c\pm d\in K\cap\mathbb{R}$．因此由引理 4.47可知 $(a+c)\pm i(b+d)\in K$．类似地，$zw=(ac-bd)+i(ad+bc)\in K$．若 $z\neq 0$，则 $z^{-1}=(a/z\bar{z})-i(b/z\bar{z})$．由 $z=a+ib\in K$ 可推出 $\bar{z}=a-ib\in K$．因此 $z^{-1}\in K$，所以 K 是 $\mathbb{C}$ 的一个子域.

若 $z=a+ib\in K$，那么由引理 4.46 可知 a，$b\in K\cap\mathbb{R}$ 和 $r^2=a^2+b^2\in K\cap\mathbb{R}$．因为 r 是非负的，所以我们有 $\sqrt{r}\in K\cap\mathbb{R}$．又 $z=re^{i\theta}$，K 是 $\mathbb{C}$ 的子域，所以 $e^{i\theta}=r^{-1}z\in K$．由每个角可以二等分得 $e^{i\theta/2}\in K$，所以 $\sqrt{z}=\sqrt{r}e^{i\theta/2}\in K$．得证. ■

推论 4.49 *若 a，b，c 是可构作的数，则二次多项式的 ax^2+bx+c 根也是可构作的数.*

证明 由二次公式和推论 4.48 即得. ■

我们现在来给出可构作数的一个代数特征．回忆，若 E/k 是一个域的扩张(即 k 为域 E 的一个子域)，E 可以看成 k 上的一个向量空间．E 的维数记为 $[E:k]$，称为 E/k 的次数．特别地，若 E/k 是一个扩张，$z\in E$ 是不可约多项式 $p(x)\in k[x]$ 的一个根，则由命题 4.30 有 $[k(z):k]=\dim_k(k(z))=\deg(p)$.

定义 *一个 **2-塔**指的是 $\mathbb{C}$ 的如下一个上升的子域塔：*

$$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n,$$

*其中对所有的 $j\geqslant 1$ 有 $[F_j:F_{j-1}]\leqslant 2$．一个复数 z 称为是**多重二次的**，如果存在一个 2-塔 $\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$ 使得 $z\in F_n$．记所由多重二次的复数构成的集合为 $\mathcal{P}$.* 359

我们从一系列引理开始，最后得到最终的结论定理 4.54：一个复数是可构作的当且仅当它是多重二次的.

引理 4.50 *若 F/k 是一个域的扩张，则 $[F:k]\leqslant 2$ 当且仅当 $F=k(u)$，其中 $u\in F$ 是某个二次多项式 $f(x)\in k[x]$ 的根.*

证明 若 $[F:k]=1$，则 $F=k$，故对所有 $u\in k$，$F=k(u)$．定义 $f(x)=(x-u)^2$．若 $[F:k]=2$，则 $F\neq k$ 且存在某 $u\in F$ 使得 $u\notin k$．由命题 4.32，存在以 u 为一根的不可约多项式 $f(x)\in$

$k[x]$. 又由定理 4.31，$2=[F:k]=[F:k(u)][k(u):k]$. 但由命题 4.30，$[k(u):k]=2$. 故$[F:k(u)]=1$，从而 $F=k(u)$.

反之，设 $F=k(u)$，其中 u 为一个二次多项式 $f(x)\in k[x]$的一根. 若 $f(x)$在 $k[x]$中可分解，则 $u\in k$，$F=k$ 且$[F:k]=1$. 若 $f(x)$不可约，则由命题 4.30，$[F:k]=[F:k(u)]=2$. ■

引理 4.51 (i)所有多重二次的复数构成的集合$\mathcal{P}$是$\mathbb{C}$的在平方根下封闭的子域.

(ii)复数 $z=a+bi$，其中 a，$b\in\mathbb{R}$，是多重二次的当且仅当 a 和 b 是多重二次的.

证明 (i)若 z，$z'\in\mathcal{P}$，则存在 2-塔$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$ 和$\mathbb{Q}(i)=F'_0\subseteq F'_1\subseteq\cdots\subseteq F'_m$且 $z\in F_n$，$z'\in F'_m$. 又$[F_j:F_{j-1}]\leqslant 2$ 推出 $F_j=F_{j-1}(u_j)$，其中 $u_j\in F_j$ 是某二次多项式 $f_j(x)\in F_{j-1}[x]$的根. 对所有的 j 有 $1\leqslant j\leqslant n$，定义 $F''_j=F'_m(u_1,\cdots,u_j)$. 因为 $F''_j=F''_{j-1}(u_j)$，所以我们有 $F_{j-1}=F'_0(u_1,\cdots,u_{j-1})\subseteq F'_m(u_1,\cdots,u_j)=F''_{j-1}$，所以 $f_j(x)\in F''_{j-1}[x]$且$[F''_j:F''_{j-1}]\leqslant 2$. 因此

$$\mathbb{Q}(i)=F'_0\subseteq F'_1\subseteq\cdots\subseteq F'_m\subseteq F''_1\subseteq\cdots\subseteq F''_n$$

为一个 2-塔. 当然 F''_n的每个元都是多重二次的. 因为 F''_n包含 z，z'，所以它包含 z 和 z'的和、积与逆. 因此$\mathcal{P}$为一个子域.

设 $z\in\mathcal{P}$. 若$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$ 是一个满足 $z\in F_n$ 的 2-塔，则$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n\subseteq F_n(\sqrt{z})$也是一个 2-塔.

(ii)若 a，$b\in\mathcal{P}$，则 $z=a+ib\in\mathcal{P}$，因为$\mathcal{P}$是包含 i 的子域. 反之，设$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$ 为使得 $z\in F_n$ 的 2-塔. 因为复共轭是$\mathbb{C}$的一个同构，所以$\mathbb{Q}(i)=\overline{F}_0\subseteq\overline{F}_1\subseteq\cdots\subseteq\overline{F}_n$ 是一个

360 满足$\overline{z}\in\overline{F_n}$的 2-塔. 因此$\overline{z}$是多重二次的，从而 $a=\frac{1}{2}(z+\overline{z})\in\mathcal{P}$且 $b=\frac{1}{2i}(z-\overline{z})\in\mathcal{P}$. ■

引理 4.52 设 $P=a+ib$ 和 $Q=c+id$ 是多重二次的.

(i)若直线 $L[P,Q]$是垂直的($c=a$)，则它的方程为 $x=a$；若它不是垂直的($c\neq a$)，则它的方程为 $y=mx+q$，其中 m，q 是多重二次的.

(ii)圆 $C[P;PQ]$的方程为$(x-a)^2+(y-b)^2=r^2$，其中 a，b，r 是多重二次的.

证明 由引理 4.51 知 a，b，c，$d\in\mathcal{P}$.

(i)若 $L[P,Q]$不是垂直的，则它的方程为 $y=mx+q$，其中 $m=(d-b)/(c-a)$及 $q=-ma+b$. 因此 m，$q\in\mathcal{P}$.

(ii)$C[P;PQ]$的方程为$(x-a)^2+(y-b)^2=r^2$，其中 r 是 P 到 Q 的距离，又 a，$b\in\mathcal{P}$，由引理 4.51，$\mathcal{P}$在平方根下是闭的，所以 $r=\sqrt{(c-a)^2+(a-b)^2}\in\mathcal{P}$. ■

命题 4.53 每个多重二次的数 z 是可构作的.

证明 若 $z\in\mathcal{P}$，则存在满足 $z\in F_n$ 的 2-塔$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$. 我们对 $n\geqslant 0$ 用归纳法来证明 $z\in K$. 由推论 4.48，$F_0=\mathbb{Q}(i)\subseteq K$，故基础步骤成立. 由于 $F_n=F_{n-1}(u)$，其中 u 是二次多项式 $f(x)=x^2+bx+c\in F_{n-1}[x]$的一个根. 二次求根公式告诉我们 $u\in F_{n-1}(\sqrt{b^2-4c})$. 由推论 4.48，$K$ 在平方根下封闭，所以$\sqrt{b^2-4c}\in K$. 由归纳假设 $F_{n-1}\subseteq K$，所以 $z\in F_{n-1}(\sqrt{b^2-4c})\subseteq K(\sqrt{b^2-4c})\subseteq K$. ■

下面是我们一直在寻找的结论.

定理 4.54 一个数 $z\in\mathbb{C}$ 是可构作的当且仅当 z 是多重二次的.

证明 由命题 4.53 知$\mathcal{P}\subseteq K$. 只须证明 $K\subseteq\mathcal{P}$，即每一个可构作的 z 是多重二次的. 设有复数 1，$w_0=-1$，w_1，…，$w_m=z$ 满足性质：对所有的 $j\geqslant 0$，w_j 可以由 w_0，w_1，…，w_{j-1} 中的点构作而得. 我们对 $m\geqslant 0$ 用归纳法来证明 w_m 是多重二次的. 因为 $w_0=-1$ 是多重二次的，故归纳的基础步骤得证. 由归纳假设，我们可设 w_0，w_1，…，w_{m-1}为多重二次的，下面证明 w_m 为多重二次的. 只须证明若 z 是由 P，Q，R，S 构作而得，其中 P，Q，R，S 是多重二次的，则 z 也是多重二次的.

情形 1 $z\in L[P,Q]\cap L[R,S]$.

若 $L[P,Q]$为垂直的，则它的方程是 $x=a$；若 $L[P,Q]$不是垂直的，那么引理 4.52 表明 $L[P,Q]$的方程是 $y=mx+q$，其中 m，$q\in\mathcal{P}$. 类似地，$L[R,S]$的方程是 $x=c$ 或 $y=m'x+p$，其中 m'，$p\in\mathcal{P}$. 因为这些直线不是平行的，所以解线性方程：

$$y=mx+q$$
$$y=m'x+p$$

得 $z=x_0+\mathrm{i}y_0\in L[P,Q]\cap L(R,S)$. 因此 $z=x_0+\mathrm{i}y_0\in\mathcal{P}$. 361

情形 2 $z\in L[P,Q]\cap C[R;RS]$.

圆 $C[R;RS]$的方程为$(x-u)^2+(y-v)^2=\rho^2$，其中 $R=(u,v)$，$S=(s,t)$，$\rho^2=(u-s)^2+(v-t)^2$. 进一步由引理 4.52 知，它的所有系数均在$\mathcal{P}$中. 若直线 $L[P,Q]$是垂直的，则它的方程是 $x=a$. 若 $z=x_0+\mathrm{i}y_0\in L[P,Q]\cap C[R;RS]$，则$(x_0-u)^2+(y_0-v)^2=\rho^2$，所以 y_0 是$\mathcal{P}[x]$上某二次多项式的根，从而 $z=a+\mathrm{i}y_0\in\mathcal{P}$. 若直线 $L[P,Q]$不是垂直的，则它的方程是 $y=mx+q$，其中 m，$q\in\mathcal{P}$. 若 $z=x_0+\mathrm{i}y_0\in L[P,Q]\cap C[R;RS]$，则$(x_0-u)^2+(mx_0+q-v)^2=\rho^2$. 因为 x_0 是$\mathcal{P}[x]$上某二次多项式的根，所以 $x_0\in\mathcal{P}$. 从而 $y_0=mx_0+q\in\mathcal{P}$和 $z=x_0+\mathrm{i}y_0\in\mathcal{P}$.

情形 3 $z\in C[P;PQ]\cap C[R;RS]$.

若 $R=(u,v)$，$S=(s,t)$，则圆 $C[R;RS]$的方程为$(x-u)^2+(y-v)^2=\rho^2$，其中 $\rho^2=(u-s)^2+(v-t)^2$. 类似地，若 $P=(a,b)$，$Q=(c,d)$，则圆 $C(P;PQ)$的方程为$(x-a)^2+(y-b)^2=r^2$，其中 $r^2=(u-s)^2+(v-t)^2$. 由引理 4.52，它们所有的系数在$\mathcal{P}$中. 若 $z=x_0+\mathrm{i}y_0\in C[P;PQ]\cap C[R;RS]$，则展开两个圆的方程即有：

$$x_0^2+y_0^2+\alpha x_0+\beta y_0+\gamma=0=x_0^2+y_0^2+\alpha' x_0+\beta' y_0+\gamma'.$$

消去 $x_0^2+y_0^2$ 得到线性方程 $\lambda x+\mu y+\nu=0$，其中 λ，μ，$\nu\in\mathcal{P}$. 事实上，$\lambda x+\mu y+\nu=0$ 是某直线 $L[P',Q']$的方程，其中 P'，$Q'\in\mathcal{P}$[例如，可取 $P'=(0,-\nu/\mu)$，$Q'=(-\nu/\lambda,0)$]，因此点 $z\in C[P;PQ]\cap C[R;RS]$就是直线 $L[P',Q']$与两个圆中的任一个的交点. 用情形 2 中的论断可以证明 $z\in\mathcal{P}$. ■

推论 4.55 若复数 z 可是可构作的，则$[\mathbb{Q}(z):\mathbb{Q}]$是 2 的方幂.

注 此推论的逆是不成立的. 可以证明存在不可构作的数 z 使得$[\mathbb{Q}(z):\mathbb{Q}]=4$. ◀

证明 由定理 4.54 和 4.31 即得. ■

注 蒙荷(G. Mohr)在 1672 年、马斯凯罗尼(L. Mascheroni)在 1797 年分别独立地证

明了每一个可由直尺和圆规构作的几何构作，不用直尺也可得到. 韩格百勒(Hungerbuhler)在《美国数学月刊》(The American Mathematical Monthly, 101(1994), 第 784 页～787 页)中给出了这个定理的一个简单的证明.

362 经典的希腊问题中有两个是被万提斯(P. L. Wantzel)在 1837 年解决的.

定理 4.56(万提斯) *仅用直尺与圆规来倍立方体是不可能的.*

证明⊖ 这个问题就是$\sqrt[3]{2}$是否是可构作的问题. 因为 x^3-2 是不可约的，由推论 4.55，$[\mathbb{Q}(z):\mathbb{Q}]=3$，但 3 不是 2 的方幂. ■

多么精巧的证明！本节开始时，我们就请求读者思考如何来证明不可能性. 这里的思想是将可构作的这个几何问题转换为一个代数的论断，再证明若存在这个构作则产生代数中的矛盾.

我教的班上有一位沉浸于科技持续发展的同学问我："是不是用直尺和圆规来倍立方永远不可能?"这个论断在字面上很清楚了：永远不可能.

定理 4.57(万提斯) *仅用直尺和圆规来三等分 60°角是不可能的.*

证明 我们不妨设这个角的一条边在 x-轴上，这样这个问题就是 $z=\cos 20°+i\sin 20°$是否是可构作的. 若 z 是可构作的，那么由引理 4.46 知 $\cos 20°$也是可构作的. 推论 1.26，即 3 倍角公式给出 $\cos 3\alpha=4\cos^3\alpha-3\cos\alpha$. 令 $\alpha=20°$，则 $\cos 3\alpha=\frac{1}{2}$. 所以 $\cos 20°$为 $4x^3-3x-\frac{1}{2}$的一个根. 等价地，$\cos 20°$为 $f(x)=8x^3-6x-1\in\mathbb{Z}[x]$一个根. 因为在模 7 下 $f(x)$是不可约的(定理 3.97)，故 $f(x)\in\mathbb{Z}[x]$在$\mathbb{Q}[x]$中是不可约的. 由定理 3.116(iv)$[\mathbb{Q}(z):\mathbb{Q}]=3$. 因为 3 不是 2 的方幂，所以 $\cos 20°$是不可构作的. ■

如果作图的规则放松，则任一角都是可三等分的.

定理 4.58(阿基米德) *每个角可以用米尺和圆规三等分，其中米尺是一条在上面能标记 U 和 V 两点，且点 U 允许在一个圆上滑动的直尺.*

证明 由于构作 30°，60°，90°等角很容易，故只须证明可三等分任一个锐角 α 即可，因为若 $3\beta=\alpha$，则 $3(\beta+30°)=\alpha+90°$，$3(\beta+60°)=\alpha+180°$且 $3(\beta+90°)=\alpha+270°$.

画一个给定的角 $\alpha=\angle AOE$，其中原点 O 为单位圆的圆心. 取一把标有长度 1 的米尺，即在米尺上有点 U 和 V 使得 $|UV|=1$. 作一条平行于 EF 的通过 A 的弦；适当放置米尺使得
363 弦就是 AU. 因为 α 是锐角，所以 U 在第一象限. 固定 A 滑动米尺使点 U 向下运动，则这米尺交延长的直径 EF 于某点 X 且 $|UX|>1$. 像在图 4-6 中一样，继续沿着圆向下移动点 U，保持 A 在滑动米尺上不动，直至米尺交 EF 于点 $X=C$(V 变成了 X).

如图 4-7，给各点重新标名，即使得 $U=B$ 且 $|BC|=1$. 我们断言 $\beta=\angle BCO=\frac{1}{3}\alpha$. 因为 α 是$\triangle AOC$ 的外角，因此它是两个相对的内角之和：

$$\alpha=\delta+\beta,$$

⊖ 在 19 世纪早期向量空间的维数不为人们所知. 作为推论 4.55 的替代，万提斯证明了，若一个数是构作的，则它是$\mathbb{Q}[x]$中某个次数为 2 的方幂的不可约多项式的根.

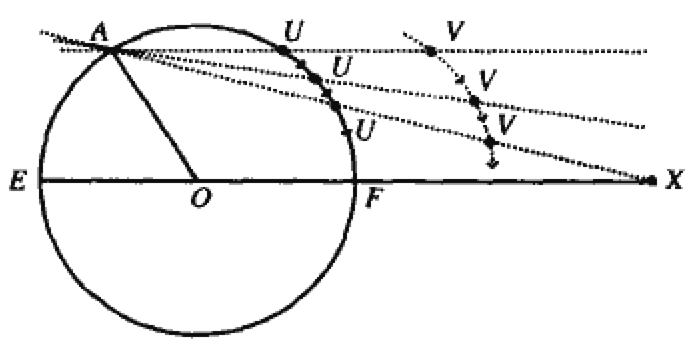


图 4-6　米尺滑动

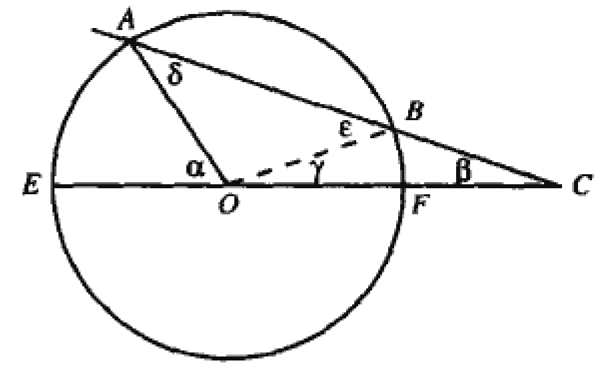


图 4-7　三等分 α

因为$\triangle OAB$是等腰三角形(OA 和 OB 是半径)，所以 $\delta=\varepsilon$. 因此

$$\alpha=\varepsilon+\beta.$$

但 $\varepsilon=\gamma+\beta=2\beta$，因为它是等腰三角形$\triangle BCO$的一个外角，所以

$$\alpha=2\beta+\beta=3\beta.$$ ■ 364

定理 4.59(林德曼)　*用直尺和圆规来化圆为方是不可能的.*

证明　这个问题就是能否构作一个正方形使得它的面积正好等于单位圆的面积. 若正方形的一条边的边长为 z，这就是问 $z=\sqrt{\pi}$是否是可构作的. 又$\mathbb{Q}(\pi)$是$\mathbb{Q}(\sqrt{\pi})$的子空间. 我们前面提到，林德曼证明了 π 是($\mathbb{Q}$ 上的)超越数，所以$[\mathbb{Q}(\pi):\mathbb{Q}]$是无限的，由推论 4.25(ii)可得$[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]$也是无限的，因此$[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]$肯定不是 2 的方幂，从而$\sqrt{\pi}$不是可构作的. ■

下面结果的充分性是高斯在大约 1796 年发现的，那时他还是一个孩子(他后来写到，正是这个结果使得他下决心成为一个数学家). 他断言必要性也是对的，但在他所有发表的论文中没有这点的完整的证明. 第一个发表的必要性的证明归功于万提斯，时间是在 1837 年.

定理 4.60(高斯-万提斯)　*设 p 为奇素数，则正 p-边形是可构作的当且仅当存在 $t\geqslant 0$ 使得 $p=2^{2^t}+1$.*

证明　只证明必要性，因为充分性见定理 5.41. 这个问题是 $z=e^{2\pi i/p}$是否是可构作的. 注意 z 是分圆多项式 $\phi_p(x)$的一个根，由推论 3.103 知分圆多项式是次数为 $p-1$ 的不可约多项式.

因为 z 是可构作的，所以 $p-1=2^s$，对某 s(由推论 4.55). 因此，

$$p=2^s+1.$$

我们来证明 s 本身也是 2 的方幂. 否则，存在奇数 $k>1$ 使得 $s=km$. k 为奇数推出而-1为 x^k+1的一个根. 事实上，在$\mathbb{Z}[x]$上有分解

$$x^k+1=(x+1)(x^{k-1}-x^{k-2}+x^{k-3}-\cdots+1).$$

令 $x=2^m$，即得 p 在$\mathbb{Z}$ 中的一个不可能的分解：

$$p=2^s+1=(2^m)^k+1=[2^m+1][(2^m)^{k-1}-(2^m)^{k-2}+(2^m)^{k-3}-\cdots+1].$$ ■

高斯直接地构作了一个正 17-边形，这是希腊人十分羡慕的功绩. 另一方面，由此得到用直尺和圆规是不可能构作如 7-边、11-边或 11-边等正多边形的.

形如 $F_t=2^{2^t}+1$ 的素数 F_t 称为**费马素数**. 对 $0\leqslant t\leqslant 4$，可以证明 F_t 是素数，事实上它们是

$$3,5,17,257 \text{ 和 } 65537.$$

接下来 t 的少量取值给出 F_t 是合数. 是否还存在其他的费马素数不得而知.

365 下面的结果是已知的.

定理 正 n-边形是可构作的当且仅当 n 是 2 的方幂与不同的费马素数的乘积.

证明 参见何罗克(Hadlock)所著的《Field theory and its Classical Problems》的第 106 页. ∎

→4.3 线性变换

向量空间之间的同态称为线性变换.

→ **定义** 称函数 $T:V\to W$ 为一个**线性变换**，其中 V 和 W 为域 k 上的向量空间，如果对所有向量 u，$v\in V$ 以及所有纯量 $a\in k$，有

(i) $T(u+v)=T(u)+T(v)$;

(ii) $T(av)=aT(v)$.

我们称线性变换 T 为**非奇异的**(或为一个**同构**)，若 T 是一个双射. 域 k 上的两个向量空间 V 和 W 是**同构的**，记为 $V\cong W$，若存在非奇异的线性变换 $T:V\to W$.

我们将很快看到线性变换是如何决定矩阵的. 推论 4.73 将证明非奇异的线性变换对应于非奇异的矩阵.

易见线性变换 T 保持所有的线性组合：

$$T(a_1v_1+\cdots+a_mv_m)=a_1T(v_1)+\cdots+a_mT(v_m).$$

→ **例 4.61** (i)任一个向量空间 V 上的恒等函数 $1_V:V\to V$ 是一个非奇异的线性变换.

(ii)若 $T:U\to V$ 是非奇异的，则它逆映射 $T^{-1}:V\to U$ 是一个线性变换且同样是非奇异的. 若 $T:U\to V$ 和 $S:V\to W$ 是线性变换，则它们的合成 $S\circ T:U\to W$ 也是一个线性变换. 若 S 和 T 都是非奇异的，则 $S\circ T$ 也是，且 $(S\circ T)^{-1}=T^{-1}\circ S^{-1}$.

(iii)设 V 和 W 为域 k 上的向量空间，记

$$\mathrm{Hom}_k(V,W)=\{V\to W \text{ 的所有线性变换}\}.$$

定义 $S+T$ 为 $S+T:v\mapsto S(v)+T(v)$，对所有的 $v\in V$. 定义 cT，其中 $c\in k$，为 $cT:v\mapsto cT(v)$，对所有的 $v\in V$. 例行的检验可以得到 $S+T$ 和 cT 都是线性变换，且 $\mathrm{Hom}_k(V,W)$ 是

366 域 k 上的一个向量空间.

(iv)设 A 是域 k 上的一个 $m\times n$ 矩阵. 易见由 $T_A(x)=Ax$ 定义的函数 $T_A:k^n\to k^m$ 是一个线性变换，其中 x 是一个 $n\times 1$ 列向量，Ax 是矩阵乘法. 在命题 4.64 中我们将看到，对某个 $m\times n$ 矩阵 A，每一个线性变换 $k^n\to k^m$ 都等于 T_A. ◀

我们现在来说明如何构造线性变换 $V\to W$，这里 V，W 为域 k 上的两个向量空间. 下一个定理指出，存在一个线性变换将基映为任一组向量. 读者应该将此定理与定理 3.33 作比较.

→ **定理 4.62** 设 v_1，…，v_n 为域 k 上的向量空间 V 的一组基. 如果 W 是域 k 上的向量空间

且 u_1，…，u_n 为 W 中的一个表，则存在唯一的满足对所有的 i 有 $T(v_i)=w_i$ 的线性变换 $T: V\to W$.

证明 由定理 4.15，每一个 $v\in V$ 都可唯一地表示为 $v=\sum_i a_iv_i$. 所以由 $T(v)=\sum_i a_iu_i$ 给出的 $T: V\to W$ 的是一个(定义良好的)函数. 经过例行的检验可以得到 T 为一个线性变换.

下面来证明 T 的唯一性. 假设 $S: V\to W$ 为一个线性变换，且满足：对所有的 i 有 $S(v_i)=w_i=T(v_i)$. 若 $v\in V$，则 $v=\sum a_iv_i$ 且

$$\begin{aligned}S(v)&=S(\sum a_iv_i)=\sum S(a_iv_i)\\&=\sum a_iS(v_i)=\sum a_iT(v_i)=T(v).\end{aligned}$$

因为 v 是任意的，所以 $S=T$. ■

→ **推论 4.63** 若线性变换 S，$T: V\to W$ 在一个基上的像相同，则 $S=T$.

证明 若 v_1，…，v_n 是 V 的一个基且对所有的 i，$S(v_i)=T(v_i)$，则定理 4.62 中的唯一性给出 $S=T$. ■

我们在定理 2.65 的证明中已经应用了此推论，定理 2.65 证明了一个正 n 边形的对称群是二面体群 D_{2n}. 平面的每一个固定原点的等距同构是一个线性变换(命题 2.59)，因此它由它在一组线性无关的两个向量组成的表上的取值确定.

线性变换 $k^n\to k^m$ 很容易描述，像在例 4.61(iv)中一样，每一个这样的线性变换都是由矩阵的乘法而产生.

→ **命题 4.64** 如果 $T: k^n\to k^m$ 是一个线性变换，则存在一个 $m\times n$ 的矩阵 A，使得对所有的 $y\in k^n$ 有

$$T(y)=Ay,$$

(这里 y 是一个 $n\times 1$ 列矩阵，Ay 是矩阵乘法). 367

证明 设 e_1，…，e_n 是 k^n 的标准基，e_1'，…，e_m' 是 k^m 的标准基. 规定 $A=[a_{ij}]$ 是它的第 j 列为 $T(e_j)$ 的坐标表的矩阵. 若 $S: k^n\to k^m$ 定义为 $S(y)=Ay$，则 $S=T$，因为它们在一个基上的取值是相同的：$T(e_j)=\sum_i a_{ij}e'_i=Ae_j=S(e_j)$，此为 A 的第 j 列.

A 的唯一性由推论 4.63 可得，因为 A 的第 j 列是 $T(e_j)$ 的坐标表. ■

设 $T: V\to W$ 为一个线性变换，$X=v_1$，…，v_n 和 $Y=w_1$，…，w_m 分别为 V 和 W 的一个基. 则 T 的矩阵由如下等式而得：

$$T(v_j)=a_{1j}w_1+a_{2j}w_2+\cdots+a_{mj}w_m=\sum_i a_{ij}w_i.$$

这就是我们记 $T(v_j)=\sum_i a_{ij}w_i$ 而不是 $T(v_j)=\sum_i a_{ji}w_i$ 的原因，这样显得更自然些.

例 4.65 我们来证明关于原点逆时针旋转 ψ 弧度的旋转 $R_\psi: \mathbb{R}^2\to\mathbb{R}^2$ 是一个线性变换. (在命题 2.59中我们给出了 R_ψ 是一个线性变换的几何证明). 若我们将$\mathbb{R}^2$ 等同于$\mathbb{C}$，则每一个点可以写成$(r\cos\theta, r\sin\theta)$(用极坐标的方式)，这样我们就有公式：

$$R_\psi(r\cos\theta, r\sin\theta)=(r\cos(\theta+\psi), r\sin(\theta+\psi)).$$

记$\mathbb{R}^2$ 的标准基为 e_1，e_2，其中

$$e_1=(1,0)=(\cos 0,\sin 0)\text{ 及 }e_2=(0,1)=(\cos\pi/2,\sin\pi/2).$$

因此，

$$R_\psi(e_1) = R_\psi(\cos 0, \sin 0) = (\cos\psi, \sin\psi),$$

以及

$$\begin{aligned} R_\psi(e_2) &= R_\psi(\cos\pi/2, \sin\pi/2) \\ &= (\cos(\pi/2+\psi), \sin(\pi/2+\psi)) \\ &= (-\sin\psi, \cos\psi). \end{aligned}$$

另一方面，若 T 为一个线性变换且满足

$$T(e_1) = (\cos\psi, \sin\psi) \text{ 及 } T(e_2) = (-\sin\psi, \cos\psi),$$

则应用余弦与正弦的加法公式有：

$$\begin{aligned} T(r\cos\theta, r\sin\theta) &= r\cos\theta T(e_1) + r\sin\theta T(e_2) \\ &= r\cos\theta(\cos\psi, \sin\psi) + r\sin\theta(-\sin\psi, \cos\psi) \\ &= (r[\cos\theta\cos\psi - \sin\theta\sin\psi], r[\cos\theta\sin\psi + \sin\theta\cos\psi]) \\ &= (r\cos(\theta+\psi), r\sin(\theta+\psi)) \\ &= R_\psi(r\cos\theta, r\sin\theta). \end{aligned}$$

368 因此 $R_\psi = T$，从而 R_ψ 为一个线性变换. ◀

下面是线性变换与矩阵间的联系.

→ **定义** 设 $X = v_1, \cdots, v_n$ 为 V 的一个基，$Y = w_1, \cdots, w_m$ 为 W 的一个基. 若 $T: V \to W$ 为一个线性变换，则 T **的关于** X **和** Y **的矩阵**就是如下的 $m \times n$ 阶矩阵 $A = [a_{ij}]$，它的第 j 列 $a_{1j}, a_{2j}, \cdots, a_{mj}$ 是 $T(v_j)$ 关于 Y 的坐标表：$T(v_j) = a_{1j}w_1 + \cdots + a_{mj}w_m$. 矩阵 A 依赖于基 X 和 Y 的选择，我们记它为

$$A = {}_Y[T]_X.$$

在 $V = W$ 情形中，我们通常假定基 $X = v_1, \cdots, v_n$ 和 $Y = w_1, \cdots, w_m$ 是一样的. 如果 $1_V: V \to V$ 为恒等线性变换，则 ${}_X[1_V]_X$ 是 $n \times n$ **单位矩阵** I_n，通常省去下标 n，记为 $I = [\delta_{ij}]$，其中 δ_{ij} 是克罗内克(Kronecker)δ 函数：

$$\delta_{ij} = \begin{cases} 0, & \text{当 } j \neq i, \\ 1, & \text{当 } j = i. \end{cases}$$

因此，I 的主对角线上元素全为 1 其余的全为 0. 另一方面，若 X 和 Y 是不同的基，则 ${}_Y[1_V]_X$ 就不是单位矩阵了，它的列是 v 关于基 Y 的坐标表(此矩阵经常称为从 X 到 Y 的**过渡矩阵**).

例 4.66 设 V 是以 $X = v_1, \cdots, v_n$ 为一个基的向量空间，$\sigma \in S_n$ 是一个置换. 由定理 4.62，存在满足对所有 i 的 $T(v_i) = v_\sigma(i)$ 线性变换 $T: V \to V$. 读者可以证明，$P_\sigma = {}_X[T]_X$ 是用 σ 置换 $n \times n$ 单位矩阵的列而得到的置换矩阵. ◀

例 4.67 设 k 是一个域，k^n 带有通常的内积：若 $v = (a_1, \cdots, a_n)$，$u = (b_1, \cdots, b_n)$，则 $(v, u) = a_1b_1 + \cdots + a_nb_n$. 定义，对所有的 u，$v \in k^n$，线性变换 $T: k^n \to k^n$ 的**伴随**[⊖]为满足

$$(Tu, v) = (u, T^* v),$$

的线性变换 $T^*: k^n \to k^n$.

⊖ 4.3 节中上有另一个伴随的概念，但与此概念无关.

我们从证明 T^* 存在开始．设 $E=e_1$，…，e_n 是标准基．若 T^* 存在，则对所有的 i，j，它不得不满足

$$(Te_j, e_i) = (e_j, T^* e_i),$$ 369

但是若 $Te_j=a_{j1}e_1+\cdots+a_{jn}e_n$，则由习题 4.14 知$(Te_j, e_i)=a_{ji}$．将此记在心上，我们定义对每个 i，$T^* e_i=a_{1i}e_1+\cdots+a_{ni}e_n$．由定理 4.62，我们就定义了一个线性变换 T^*．

若 $A=[a_{ij}]={}_E[T]_E$，则 T^* 的定义等式表明${}_E[T^*]_E=A^T$，也就是，T 的伴随矩阵是 A 的转置．

伴随的定义可以推广．若 $T: V\to W$ 是一个线性变换，其中 V 和 W 是带有内积的向量空间．则它的伴随为对所有的 $v\in V$，$w\in W$，满足$(Tv, w)=(v, T^* w)$的线性变换 $T^*: W\to V$． ◀

例 4.68 (i)在例 4.68 中，我们考虑了 $R_\psi: \mathbb{R}^2\to\mathbb{R}^2$，关于原点逆时针旋转 ψ 弧度的旋转．R_ψ 关于标准基 e_1，e_2 的矩阵是

$${}_E[R_\psi]_E = \begin{bmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{bmatrix}.$$

(ii)此例表明对于给定的线性变换，其相应的矩阵可以不同．设 $T: \mathbb{R}^2\to\mathbb{R}^2$ 是关于原点逆时针旋转$\frac{\pi}{2}$弧度的旋转．同(i)中一样，T 关于标准基 $X=e_1$，e_2 的矩阵是

$${}_X[T]_X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

表 $Y=v_1$，v_2 是一个基，其中 $v_1=(4, 1)^T$，$v_2=(-2, 1)^T$ 是行向量．我们通过将 $T(v_1)$ 和 $T(v_2)$写成 v_1，v_2 的线性组合来计算${}_Y[T]_Y$．而

$$T(v_1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 4 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 4 \end{bmatrix},$$

$$T(v_2) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -2 \\ 1 \end{bmatrix} \begin{bmatrix} -1 \\ -2 \end{bmatrix}.$$

我们必须求满足

$$T(v_1) = \begin{bmatrix} -1 \\ 4 \end{bmatrix} = av_1 + bv_2,$$

$$T(v_2) = \begin{bmatrix} -1 \\ -2 \end{bmatrix} = cv_1 + dv_2.$$

的数 a，b，c，d．

每个向量方程给出了一个线性方程组：

$$4a - 2b = -1$$
$$a + b = 4$$ 370

和

$$4c - 2d = -1$$
$$c + d = -2$$

易解得：

$$a=\frac{7}{6},\quad b=\frac{17}{6},\quad c=-\frac{5}{6},\quad d=-\frac{7}{6}.$$

从而

$$_Y[T]_Y=\frac{1}{6}\begin{bmatrix}7 & -5\\ 17 & -7\end{bmatrix}.$$

此计算在例 4.75 中将再一次看到. ◀

例 4.69 对给定的一个线性变换 $T:V\to V$ 和 V 的一组基 X，我们已经解释了如何建立矩阵 $A={}_X[T]_X$. 现在我们将此过程反过来并证明如何从 k 上的一个 $n\times n$ 矩阵来构造一个线性变换.

考虑矩阵

$$C=\begin{bmatrix}0 & 0 & 8\\ 1 & 0 & -6\\ 0 & 1 & 12\end{bmatrix}.$$

为定义一个线性变换 $T:k^3\to k^3$，只需对每一个在标准基 $E=e_1$，e_2，e_3 中的向量 e_i 给定 $T(e_i)$ 即可. 用 C 的列，我们定义

$$T(e_1)=e_2,T(e_2)=e_3,T(e_3)=8e_1-6e_2+12e_3.$$

当然，$C={}_E[T]_E$.

我们现在来求 T 关于一组新基的矩阵. 定义 $X=x_0$，x_1，x_2 为

$$x_0=e_1,x_1=(C-2I)e_1,x_2=(C-2I)^2e_1.$$

我们通过证明 $\langle X\rangle=k^3$ 来证明 X 生成 k^3. 显然，$e_1=x_0\in\langle X\rangle$，而 $x_1=Ce_1-2e_1=e_2-2x_0$，因此

$$e_2=2x_0+x_1\in\langle X\rangle.$$

又 $x_2=C^2e_1-4Ce_1+4e_1=e_3-4e_2+4e_1$，所以

$$\begin{aligned}e_3&=x_2+4e_2-4e_1\\&=x_2+4(2x_0+x_1)-4x_0\\&=4x_0+4x_1+x_2\in\langle X\rangle.\end{aligned}$$

371

在一个 3 维向量空间中，3 个向量组成的一个张成 V 的表一定是一组基，因此 X 是 k^3 的一组基.

矩阵 $J={}_X[T]_X$ 是什么？用前面的方程，读者可验证

$$\begin{aligned}T(x_0)&=2x_0+x_1\\T(x_1)&=2x_1+x_2\\T(x_2)&=2x_2.\end{aligned}$$

由此得出 T 关于基 X 的矩阵是

$$J=\begin{bmatrix}2 & 0 & 0\\ 1 & 2 & 0\\ 0 & 1 & 2\end{bmatrix}.$$ ◀

下面命题是定理 4.62 的一个解释.

→ **命题 4.70** 设 V 和 W 是域 k 上的向量空间，X 和 Y 分别是 V 和 W 的基. 则由

$$T \mapsto {}_Y[T]_X$$

给出的函数

$$\mu_{X,Y}: \mathrm{Hom}_k(V,W) \to \mathrm{Mat}_{m\times n}(k)$$

是一个向量空间的同构.

证明 首先我们来证明 $\mu_{X,Y}$ 是一个满射. 给定一个矩阵 A，用它的行来定义 W 中的向量. 详细来说，若 $X=v_1, \cdots, v_n$ 和 $Y=w_1, \cdots, w_m$，则 A 的第 j 行是 $(a_{1j}, \cdots, a_{mj})^{\mathrm{T}}$. 定义 $z_j = \sum_{i=1}^{m} a_{ij} w_i$. 由定理 4.62 知，存在满足 $T(v_j)=z_j$ 和 ${}_Y[T]_X=A$ 的一个线性变换 $T: V\to W$. 为证明 $\mu_{X,Y}$ 是一个单射，假设 ${}_Y[T]_X=A={}_Y[S]_X$. 因为对所有 j，A 的行决定了 $T(v_j)$ 和 $S(v_j)$，由推论 4.63 知 $S=T$.

最后，我们来证明 $\mu_{X,Y}$ 是一个线性变换. 因为对所有的 j，$S+T$ 的第 j 行是 $(S+T)(v_j)=S(v_j)+T(v_j)$，所以我们有 $\mu_{X,Y}(S+T)=\mu_{X,Y}(S)+\mu_{X,Y}(T)$. 类似的论断表明 $\mu_{X,Y}(cT)=c\mu_{X,Y}(T)$. ■

下面的定理表明了矩阵乘法定义的出处：两个矩阵的乘积是两个线性变换合成的矩阵.

→ **定理 4.71** 设 $T: V\to W$ 和 $S: W\to U$ 为两个线性变换. 取 V 的一组基 $X=x_1, \cdots, x_n$，W 的一组基 $Y=y_1, \cdots, y_m$ 和 U 的一组基 $Z=z_1, \cdots, z_l$，则

$${}_Z[S\circ T]_X = ({}_Z[S]_Y)({}_Y[T]_X).$$ 372

证明 设 ${}_Y[T]_X=[a_{ij}]$，这样 $T(x_j)=\sum_p a_{pj}y_p$. ${}_Z[S]_Y=[b_{qp}]$，这样 $S(y_p)=\sum_q b_{qp}z_q$. 则

$$\begin{aligned}(S\circ T)(x_j) = S(T(x_j)) &= S\Big(\sum_p a_{pj}y_p\Big)\\ &= \sum_p a_{pj}S(y_p) = \sum_p\sum_q a_{pj}b_{qp}z_q = \sum_q c_{qj}z_q,\end{aligned}$$

其中，$c_{qj}=\sum_p b_{qp}a_{pj}$. 因此，

$${}_Z[S\circ T]_X = [c_{qj}] = ({}_Z[S]_Y)({}_Y[T]_X).$$ ■

推论 4.72 矩阵的乘法满足结合律：$A(BC)=(AB)C$.

证明 设 A 为一个 $m\times n$ 的矩阵，B 为一个 $n\times p$ 的矩阵，而 C 为一个 $p\times q$ 的矩阵. 由定理 4.62 知，存在满足 $C=[T]$，$B=[S]$ 和 $A=[R]$（为使证明不杂乱，我们将记号中的基省略：我们记为 $[T]$ 而不是 ${}_Y[T]_X$）的线性变换

$$k^q \xrightarrow{T} k^p \xrightarrow{S} k^n \xrightarrow{R} k^m.$$

则

$$[R\circ(S\circ T)] = [R][S\circ T] = [R]([S][T]) = A(BC).$$

另一方面，

$$[(R\circ S)\circ T] = [R\circ S][T] = ([R][S])[T] = (AB)C.$$

因为函数的复合满足结合律，

$$R\circ(S\circ T) = (R\circ S)\circ T.$$

所以

$$A(BC)=[R\circ(S\circ T)]=[(R\circ S)\circ T]=(AB)C.$$ ■

我们也可以直接证明推论 4.72：巧妙地处理求和，但与线性变换合成的联系是矩阵乘法满足结合律的真正原因.

推论 4.73 设 $T:V\to W$ 是域 k 上向量空间 V 和 W 的一个线性变换，X 和 Y 分别是 V 和 W 的基. 若 T 为非奇异的且 $A={}_Y[T]_X$，则 A 是一个非奇异的矩阵且

$${}_X[T^{-1}]_Y=A^{-1}=({}_Y[T]_X)^{-1}.$$

反之，若对 V 的某组基 X 和 W 的某组基 W，$A={}_Y[T]_X$ 是一个非奇异的矩阵，则 T 是一个非

373 奇异的线性变换.

证明

$$I={}_Y[1_W]_Y=({}_Y[T]_X)({}_X[T^{-1}]_Y)$$

和

$$I={}_X[1_V]_X=({}_X[T^{-1}]_Y)({}_Y[T]_X).$$

因此，${}_X[T^{-1}]_Y=({}_Y[T]_X)^{-1}$.

设 $B=[b_{ij}]$是一个满足 $BA=I=AB$ 的矩阵. 同在定理 4.62 中一样，存在满足 $S(y_i)=\sum_p b_{pi}x_p$ 的唯一一个线性变换 $S:W\to V$. 由 B 关于基 Y 和 X 的矩阵的定义，我们有 $B={}_X[S]_Y$. 因此，

$$I=BA={}_X[S]_Y\,{}_Y[T]_X={}_X[S\circ T]_X.$$

从而对所有的 i 有$(S\circ T)(x_i)=Ix_i=x_i$，故 $S\circ T=1_V$. 应用 $I=AB$，类似的论断可以证明 $T\circ S=1_W$. 我们得出结论 T 是一个双射，因此它是一个非奇异的线性变换. ■

下面的推论确定了从同一个线性变换而得的所有矩阵.

→ **推论 4.74** 设 $T:V\to V$ 是域 k 上向量空间 V 的一个线性变换，X 和 Y 分别是 V 的基，则存在一个元素在 k 中的非奇异的矩阵 P，也就是 $P={}_Y[1_V]_X$，使得

$${}_Y[T]_Y=P({}_X[T]_X)P^{-1}.$$

反之，若 $B=PAP^{-1}$，其中 A，B 和 P 是元素在 k 中的矩阵，P 是非奇异的，则存在一个线性变换 $T:k^n\to k^n$ 和 k^n 的基 X 和 Y 使得 $B={}_Y[T]_Y$ 和 $A={}_X[T]_X$.

证明 第一部分由定理 4.71 和矩阵的结合律可得：

$${}_Y[T]_Y={}_Y[1_VT1_V]_Y=({}_Y[1_V]_X)({}_X[T]_X)({}_X[1_V]_Y).$$

记 $P={}_Y[1_V]_X$. 注意推论 4.73 给出了 $P^{-1}={}_X[1_V]_Y$.

为证明逆命题，设 $E=e_1,\cdots,e_n$ 为 k^n 的标准基，定义 $T:k^n\to k^n$ 为 $T(e_j)=Ae_j$(记住，k^n 中的向量是列向量，所以 Ae_j 是矩阵乘法). 因为 Ae_j 是 A 的第 j 行，所以我们有 $A={}_E[T]_E$. 定义一个表 $Y=y_1,\cdots,y_n$，其中 $y_j=P^{-1}e_j$，即，Y 中的向量是 P^{-1}的列向量.

我们来证明 $Y=P^{-1}e_1,\cdots,P^{-1}e_n$ 是 k^n 的一个基. 若 $\sum_j a_jP^{-1}e_j=0$,则 $P^{-1}\left(\sum_j a_je_j\right)=0$.

374 在左边乘上 P 得到 $\sum_j a_je_j=0$,标准基的线性无关性给出所有 $a_j=0$. 因此Y是线性无关的. 为证

明 Y 张成 k^n，取 $w \in k^n$. 又 $Pw = \sum_j b_j e_j$，故 $w = P^{-1}Pw = \sum_j b_j P^{-1} e_j \in \langle Y \rangle$. 从而 Y 是一个基.

现在只剩下要证明 $B = {}_Y[T]_Y$，即 $T(y_j) = \sum_i b_{ij} y_i$，其中 $B = [b_{ij}]$.

$$\begin{aligned} T(y_j) &= Ay_j = AP^{-1}e_j = P^{-1}Be_j \\ &= P^{-1}\sum_i b_{ij}e_i = \sum_i b_{ij}P^{-1}e_i = \sum_i b_{ij}y_i. \end{aligned}$$ ■

→ **定义** 域 k 上两个 $n \times n$ 矩阵 A 和 B 称为是**相似的**，若存在 k 上一个非奇异的矩阵 P 使得 $B = PAP^{-1}$.

推论 4.74 说两个矩阵是相似的当且仅当它们是从向量空间 V 的同一个线性变换而得的矩阵(由基的不同选择而得). 例如，在例 4.69 中，矩阵 C 和 J 是相似的. 第一个矩阵 C 是从一个线性变换 $T: k^3 \to k^3$ 关于标准基 E 而得的，即 $C = {}_E[T]_E$. 在例子中，第二个矩阵 J 是从该线性变换关于基 X 而得的，即 $J = {}_X[T]_X$.

例 4.75 我们现在来简化例 4.68(ii)中的计算. 回忆到我们已经有$\mathbb{R}^2$ 的两个基：标准基 $E = e_1$，e_2 和 $F = v_1$，v_2，其中 $v_1 = \begin{bmatrix} 4 \\ 1 \end{bmatrix}$，$v_2 = \begin{bmatrix} -2 \\ 1 \end{bmatrix}$及线性变换 $T: \mathbb{R}^2 \to \mathbb{R}^2$，关于原点逆时针旋转$\frac{\pi}{2}$弧度的旋转，其矩阵为

$${}_E[T]_E = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

过渡矩阵为

$$P^{-1} = {}_E[1]_F = \begin{bmatrix} 4 & -2 \\ 1 & 1 \end{bmatrix}$$

和

$$P = {}_F[1]_E = {}_E[1]_F^{-1} = \frac{1}{6}\begin{bmatrix} 1 & 2 \\ -1 & 4 \end{bmatrix}.$$

因此，

$${}_F[T]_F = P_E[T]_E P^{-1} = \frac{1}{6}\begin{bmatrix} 7 & -5 \\ 17 & -7 \end{bmatrix},$$

这与 4.3 节中的结果一样. ◀

如同群同态和环同态一样，我们可以定义线性变换的核与象. 375

定义 设 $T: V \to W$ 是一个线性变换，则 T 的**核**(或**零空间**)规定为：

$$\ker T = \{v \in V : T(v) = 0\},$$

T 的**象**规定为：

$$\operatorname{im} T = \{w \in W: \text{存在某个 } v \in V \text{ 使得 } w = T(v)\}.$$

同例 4.7(ii)中一样，一个元素在域 k 中的 $m \times n$ 的矩阵决定了一个线性变换 $T_A: k^n \to k^m$，也就是 $T_A(y) = Ay$，这里 y 是一个 $n \times 1$ 的列向量. T_A 的核为解空间 $Sol(A)$[参见例 4.3(iv)]，T_A 的象为行空间 $\mathrm{Col}(A)$.

下面的命题的证明是直接的.

命题 4.76 设 $T: V \to W$ 为一个线性变换.

(i) $\ker T$ 是 V 的一个子空间，而 $\mathrm{im} T$ 是 W 一个子空间.

(ii) T 是单射当且仅当 $\ker T = \{0\}$.

我们现在可以给出推论 4.20 的一个新证明. 推论 4.20 说，域 k 上的 r 个方程 n 个未知量的齐次方程组有非平凡的解若 $r<n$. 若 A 是此方程组的 $r \times n$ 的系数矩阵，则 $T: x \mapsto Ax$ 是一个线性变换 $T: k^n \to k^r$. 若只有平凡的解，则 $\ker T = \{0\}$，因此 k^n 与子空间 $\mathrm{im} T \subseteq k^r$ 同构，这与推论 4.25(ii)矛盾.

引理 4.77 下列关于线性变换 $T: V \to W$ 的论断是等价的.

(i) T 是非退化的(即 T 是一个同构).

(ii) 对 V 的每一个基 X，我们有 $T(X)$ 也是 W 的一个基.

(iii) 对 V 的某一个基 X，$T(X)$ 是 W 的一个基.

证明 (i)⇒(ii). 设 $X = v_1, \cdots, v_n$ 为 V 的一个基. 若 $\sum c_i T(v_i) = 0$，则 $T(\sum c_i v_i) = 0$，所以 $\sum c_i v_i \in \ker T = \{\}0$，因此 $\sum c_i v_i = 0$. 因为 X 是线性无关的，从而对每一个 i 有 $c_i = 0$. 若 $w \in W$，因为 T 为满射，所以存在 $v \in V$ 使得 $w = T(v)$. 但 $v = \sum a_i v_i$，所以 $w = T(v) = T(\sum a_i v_i) = \sum a_i T(v_i)$. 因此 $T(X)$ 为 W 的一个基.

(ii)⇒(iii). 显然.

(iii)⇒(i). 若 $w \in W$，因为 $T(v_1), \cdots, T(v_n)$ 是 W 的一组基，故 $w = \sum c_i T(v_i) = T(\sum c_i v_i)$，所以 T 是一个满射. 若 $\sum c_i v_i \in \ker T$，则 $\sum c_i T(v_i) = 0$. $T(v_1), \cdots, T(v_n)$ 的线性
376 无关性推出所有的 $c_i = 0$. 因此 $\sum c_i v_i = 0$，$\ker T = \{0\}$. 从而 T 是一个单射. ■

→ **定理 4.78** 若 V 是域 k 上的 n 维向量空间，则 V 同构于 k^n.

证明 取定 V 的一个基 $v_1, \cdots, v_n$. 设 $e_1, \cdots, e_n$ 为 k^n 的一个标准基，由定理 4.62 知，存在线性变换 $T: V \to k^n$ 使得对所有的 i 有 $T(v_i) = e_i$. 由引理 4.77 知，T 是非退化的. ■

定理 4.78 不仅仅告诉我们每一个有限维向量空间本质上是我们所熟悉的 n 元有序元素组构成的向量空间，而且告诉我们 V 的基的选择等价于对每个向量其坐标的选择. 人们想自由地改变坐标，因为对给定的问题通常的坐标有可能不是最方便的，读者也许注意到(在微积分课程中)旋转轴的采用可以简化二次曲线的方程.

→ **推论 4.79** 域 k 上的两个有限维向量空间 V 和 W 是同构的当且仅当 $\dim(V) = \dim(W)$.

证明 假设存在一个非退化的线性变换 $T: V \to W$. 若 $X = v_1, \cdots, v_n$ 是 V 的一个基，则由引理 4.77 可知，$T(v_1), \cdots, T(v_n)$ 是 W 的一个基. 因此 $\dim(W) = |X| = \dim(V)$.

若 $n = \dim(V) = \dim(W)$，则由定理 4.78 可知，存在同构 $T: V \to k^n$ 及 $S: W \to k^n$. 从而合成 $S^{-1} \circ T: V \to W$ 是非退化的. ■

→ **命题 4.80** 设 V 是域 k 上的一个有限维向量空间，$\dim(V) = n$，$T: V \to V$ 是一个线性变换. 下列论断是等价的.

(i) T 是一个同构.

(ii) T 是一个满射.

(iii)T 是一个单射.

注 将此命题与习题 2.13 的鸽巢原理作比较.

证明 (i)⇒(ii). 此推理是显然的，因为同构是一个双射.

(ii)⇒(iii). 假设 T 是一个满射. 若 $X=v_1, \cdots, v_n$ 为 V 的一个基，我们断言 $T(X)=T(v_1), \cdots, T(v_n)$张成$V$. 若 $w\in V$，则 T 的满射给出 $v\in V$ 使得 $w=T(v)$. 又 $v=\sum_i a_iv_i$，对某些纯量 $a_i\in k$，故 $w=T(v)=\sum_i a_iT(v_i)$. 因为 $\dim(V)=n$，所以由推论 4.42 得出 $T(X)$是 V 的一个基. 引理 4.77 说 T 是一个同构，故 T 是一个单射. 377

(iii)⇒(i). 假设 T 是单射. 若 $X=v_1, \cdots, v_n$ 为 V 的一组基，我们断言 $T(X)=T(v_1), \cdots, T(v_n)$是线性无关的. 若$\sum c_iT(v_i)=0$，则 $T(\sum_i c_iTv_i)=0$，故$\sum_i c_iv_i\in\ker T=\{0\}$. 因此$\sum_i c_iv_i=0$. X 的线性无关性给出 $c_i=0$，从而 $T(X)$是线性无关的. 因为 $\dim(V)=n$，由推论 4.24 得出 $T(X)$是 V 的一个基. 引理 4.77 说 T 是一个同构. ■

称线性变换 $T: V\to V$ 是**奇异的**若 T 不是一个同构，即 T 不是非奇异的.

推论 4.81 设 V 是一个有限维向量空间，$T: V\to V$ 是一个线性变换. T 是奇异的当且仅当存在一个满足 $T(v)=0$ 的非零向量 $v\in V$.

证明 若 T 是奇异的，则由命题 4.80 得 $\ker T\neq\{0\}$. 反之，若存在一个满足 $T(v)=0$ 的非零向量 $v\in V$，则 $\ker T\neq\{0\}$，从而 T 不是一个同构. ■

此推论说一个具有奇异的系数矩阵 A 的齐次线性方程组 $Ax=0$ 总是有非平凡的解.

回忆元素在域 k 中的一个 $n\times n$ 的矩阵 A 是非退化的，若存在一个含有域 k 中的元素的矩阵 B(它的逆)使得 $AB=I=BA$. 下推论表明“单边可逆”就足够了.

推论 4.82 设 A 和 B 是元素在域 k 中的 $n\times n$ 的矩阵. 若 $AB=I$，则 $BA=I$. 从而 A 是非奇异的且 $B=A^{-1}$.

证明 存在满足${}_X[T]_X=A$ 和${}_X[S]_X=B$ 的线性变换 $T, S: k^n\to k^n$，其中 X 是标准基. 在此证明中，我们将${}_X[T]_X$ 简记为$[T]$. 因为 $AB=I$，由命题 4.70，

$$[T\circ S]=[T][S]=I=[1_{k^n}].$$

因为 $T\mapsto[T]$是一个双射，由命题 4.70 得出 $T\circ S=1_{k^n}$. 由命题 2.9，T 是一个满射，S 是一个单射. 但命题 4.80 说 T 和 S 都是同构，所以 $S=T^{-1}$ 且 $T\circ S=1_{k^n}=S\circ T$. 从而 $I=[S\circ T]=[S][T]=BA$，得证. ■

→ **命题 4.83** 设 $T: V\to W$ 为一个线性变换，其中 V 和 W 是域 k 上维数分别为 n 和 m 的向量空间. 则

$$\dim(\ker T)+\dim(\operatorname{im} T)=n.$$

证明 选择 $\ker T$ 的一个基 $u_1, \cdots, u_p$，并通过添加向量 $w_1, \cdots, w_q$ 将之扩充为 V 的一个基. 因为 V 由表 $u_1, \cdots, u_p, w_1, \cdots, w_q$ 张成，子空间 $\operatorname{im}T$ 由表 $T(u_1), \cdots, T(u_p)$, 378
$T(w_1), \cdots, T(w_q)$张成. 而对所有的 i 有 $T(u_i)=0$，因此 $\operatorname{im}T$ 由更短的表 $T(w_1), \cdots, T(w_q)$ 张成. 因为 $\dim(\ker T)=p$ 和 $p+q=n$，故只须证明 $T(w_1), \cdots, T(w_q)$是一个线性无关的表即可.

若 $c_1T(w_1)+\cdots+c_qT(w_q)=0$，则 $T(c_1w_1+\cdots+c_qw_q)=0$，即，$c_1w_1+\cdots+c_qw_q\in\ker T$. 因此存在 a_1，…，$a_p\in k$ 使得

$$c_1w_1+\cdots+c_qw_q = a_1u_1+\cdots+a_pu_p.$$

因为 u_1，…，u_p，w_1，…，w_q 是 V 的一个基，它是一个线性无关的表，所以 $0=c_1=\cdots=c_q$（当然 $0=a_1=\cdots=a_p$）．从而 $T(w_1)$，…，$T(w_q)$是 $\operatorname{im}T$ 的一个基且 $\dim(\operatorname{im}T)=q$. ■

→ **推论 4.84** 设 A 是在域 k 中的一个 $m\times n$ 矩阵.

(i)$\operatorname{rank}(A)=\dim(\operatorname{im}T_A)$，其中 $T_A: k^n\to k^m$ 由 $T_A(x)=Ax$ 定义.

(ii)$\operatorname{rank}(A)=\dim(\operatorname{Col}(A))$.

(iii)$\operatorname{rank}(A)=\operatorname{rank}(A^T)$，即，$\operatorname{Row}(A)$和 $\operatorname{Col}(A)$有相同的维数.

证明 (i)由定理 4.43 秩-零化度定理，$\dim(\operatorname{Sol}(A))=n-\operatorname{rank}(A)$，也就是 $\operatorname{rank}(A)=n-\dim(\operatorname{Sol}(A))$. 但 $\ker T_A=\operatorname{Sol}(A)$. 故由命题 4.83，$\dim(\operatorname{im}T_A)=n-\dim(\operatorname{Sol}(A))=\operatorname{rank}(A)$.

(ii)$\operatorname{im}T_A=\langle T_A(e_1),\cdots,T_A(e_n)\rangle=\langle Ae_1,\cdots,Ae_n\rangle=\operatorname{Col}(A)$.

(iii)由定义，$\operatorname{rank}(A)=\dim(\operatorname{Row}(A))$，而 $\operatorname{rank}(A)=\dim(\operatorname{Col}(A))$在(ii)中已证. ■

→ **定义** 设 V 为域 k 上的一个向量空间. 所有非奇异的线性变换 $V\to V$ 组成的集合称为**一般线性群**，记为 $GL(V)$.

线性变换 S 和 T 的合成$S\circ T$也是一个线性变换. 若 S 和 T 都是非奇异，则 $S\circ T$ 也是非奇异的. 进一步，一个非奇异的线性变换的逆映射还是非奇异的. 由此得出 $GL(V)$以线性变换的合成作为运算构成一个群，因为函数的合成总是满足结合律.

→ **定义** 元素在域 k 中的所有非奇异的 $n\times n$ 的矩阵构成的集合记为 $GL(n, k)$.

易证 $GL(n, k)$以矩阵的乘法作运算构成一个群.

379 基的选择给出了一般线性群与非奇异的矩阵群之间的同构.

→ **命题 4.85** 设 V 为域 k 上的一个 n 维向量空间，$X=v_1$，…，v_n 是 V 的一个基. 则由 $T\mapsto {}_X[T]_X$ 定义的 $\mu: GL(V)\to GL(n, k)$是一个群同构.

证明 由命题 4.70，函数 $\mu_{X,X}: T\mapsto[T]={}_X[T]_X$ 是向量空间

$$\operatorname{Hom}_k(V,V)\to\operatorname{Mat}_n(k)$$

的一个同构. 进一步，由定理 4.71，对所有的 T，$S\in\operatorname{Hom}_k(V, V)$，$\mu_{X,X}(T\circ S)=\mu_{X,X}(T)\mu_{X,X}(S)$.

若 $T\in GL(V)$，则由推论 4.73，$\mu_{X,X}(T)={}_X[T]_X$ 是一个非奇异的矩阵. 因此，若 μ 是 $\mu_{X,X}$的限制，则 $\mu: GL(V)\to GL(n, k)$是一个单射同态.

现在只剩下证明μ是一个满射了. 因为 $\mu_{X,X}$是满射，所以若 $A\in GL(n, k)$，则有某 $T: V\to V$ 使得 $A={}_X[T]_X$. 只须证明 T 是一个同构，因为这样的话就有 $T\in GL(V)$. 因为 A 是一个非奇异的矩阵，所以存在矩阵 B 使得 $AB=I$. 又有某 $S: V\to V$ 使得 $B={}_X[S]_X$，且

$$\mu_{X,X}(T\circ S)=\mu_{X,X}(T)\mu_{X,X}(S)=AB=I=\mu_{X,X}(1_V).$$

从而，$T\circ S=1_V$. 因为 $\mu_{X,X}$是一个单射，所以由推论 4.82 有 $T\in GL(V)$. ■

一般线性群的中心很容易确定；现在我们来推广习题 2.84.

定义 线性变换 $T: V\to V$ 称为是一个**纯量变换**，如果存在 $c\in k$ 使得对所有的 $v\in V$，有 $T(v)=cv$，即 $T=c1_V$. 一个**纯量矩阵**是一个形如 cI 的矩阵，其中 $c\in k$ 且 I 是单位矩阵.

纯量变换 $T=c1_V$ 是非奇异的当且仅当 $c\neq 0$（它的逆映射是 $c^{-1}1_V$）.

推论 4.86 群 GL(V)的中心由所有的非奇异的纯量变换组成. 群 GL(n, k)的中心由所有的非奇异的纯量矩阵组成.

证明 若 $T\in \mathrm{GL}(V)$ 不是纯量变换，则存在 $v\in V$ 使得 $T(v)$ 不是 v 的纯量倍. 当然有 $v\neq 0$. 我们断言 $X=v$，我们知道 $T(v)$ 不是 v 的纯量倍. 若对 $d\in k$ 有 $v=dT(v)$，则 $d\neq 0$（除非 $v=0$），所以 $T(v)=d^{-1}v$，矛盾！因此由习题 4.12(iii)知，v，$T(v)$是一个线性无关的表。由命题 4.22，可将之扩充为 V 的一个基 v，$T(v)$，u_3，…，u_n. 易见 v，$v+T(v)$，u_3，…，u_n 也是 V 的一个基，所以存在一个非奇异的线性变换 S 满足 $S(v)=v$，$S(T(v))=v+T(v)$ 且对所 380
有的 i 有 $S(u_i)=u_i$. 注意 S 与 T 是不可换的，因为 $ST(v)=v+T(v)$，而 $TS(v)=T(v)$. 从而 T 不在 GL(V)的中心内.

若 $f:G\to H$ 是群 G 与 H 之间的一个群同构映射，则 $f(Z(G))=Z(H)$. 易见，若 $T=c1_V$ 为一个纯量变换，则对 V 的任意一个基 v_1，…，v_n，${}_X[T]_X$ 在 GL(n, k)的中心内. 由于对所有的 i 有 $T(v_i)=v_i$，故 ${}_X[T]_X=cI$ 是一个纯量矩阵. ■

习题

H 4.32 判断对错并说明理由.

(i)每一个线性变换 $T:V\to V$，其中 V 是$\mathbb{R}$上的一个有限维向量空间，可用无数个矩阵来表示.

(ii)$\mathbb{R}$上每一个矩阵都相似于无数个不同的矩阵.

(iii)若 S 和 T 是平面$\mathbb{R}^2$ 上的线性变换，且它们在两个非零点处相等，则 $S=T$.

(iv)若 A 和 B 是 $n\times n$ 非奇异的矩阵，则 $A+B$ 也是非奇异的.

(v)若 A 和 B 是 $n\times n$ 非奇异的矩阵，则 AB 也是非奇异的.

(vi)设 k 是一个域，则

$$\{A\in \mathrm{Mat}_n(k): AB=BA, \text{对所有的 } B\in \mathrm{Mat}_n(k)\}$$

是 $\mathrm{Mat}_n(k)$的 1 维子空间.

(vii)$\mathbb{R}$上所有 3×3 的对称矩阵构成的向量空间同构于由 0 及所有满足 $\deg(f)\leqslant 5$ 的 $f(x)\in\mathbb{R}[x]$组成的向量空间.

(viii)设 X 和 Y 是域 k 上有限维向量空间 V 的基，则${}_Y[1_V]_X$ 是单位矩阵.

(ix)由 $A\mapsto A^{\mathrm{T}}$ 给出的变换 $\mathrm{Mat}_{n\times m}(\mathbb{C})\to \mathrm{Mat}_{n\times m}$是非退化的线性变换.

(x)设 V 是所有连续函数 $f:[0,1]\to\mathbb{R}$ 组成的向量空间，则积分 $f\mapsto \int_0^1 f(x)\mathrm{d}x$ 是一个线性变换.

4.33 设 K 是一个域，多项式环 $V=k[x]$被视为 k 上的向量空间且 $V_n=\langle 1, x, x^2, \cdots, x^n\rangle$. 由习题 4.8，我们知道 $X_n=1$，x，x^2，…，x^n 是 V 的一个基.

(i)证明由 $T(f(x))=f'(x)$定义的微分 $T:V_3\to V_3$ 是一个线性变换且求微分的矩阵 $A={}_{X_3}[T]_{X_3}$.

(ii)证明由 $S(f)=\int_0^x f(t)\mathrm{d}t$ 定义的积分是一个线性变换且求积分的矩阵 $A={}_{X_4}[S]_{X_3}$.

4.34 设 $\sigma\in S_n$，$P=P_\sigma$ 是相应的置换矩阵（参见例 4.66），试证 $P^{-1}=P^{\mathrm{T}}$. 381

*4.35 设 V 和 W 为域 k 上的向量空间. 设 S，$T:V\to W$ 为线性变换.

(i)若 V 和 W 是有限维向量空间，试证

$$\dim(\mathrm{Hom}_k(V,W))=\dim(V)\dim(W).$$

(ii)域 k 上向量空间 V 的对偶空间 V^* 定义为

$$V^* = \mathrm{Hom}_k(V, k).$$

若 $X = v_1, \cdots, v_n$ 为 V 的一个基，定义 $\delta_1, \cdots, \delta_n \in V^*$ 为

$$\delta_i(v_j) = \begin{cases} 0, & 当\ j \neq i, \\ 1, & 当\ j = i. \end{cases}$$

试证 $\delta_1, \cdots, \delta_n$ 为 V 的一个基(称为由 $v_1, \cdots, v_n$ 而得的对偶基).

(iii)若 $\dim(V^*) = n$，试证 $V^* \cong V$.

*4.36 (i)若 $S: V \to W$ 是一个线性变换，$f \in W^*$. 则合成 $V \xrightarrow{S} W \xrightarrow{f} k$ 是落在 V^* 中的. 试证由 $S^*: f \mapsto f \circ S$ 定义的 $S^*: W^* \to V^*$ 是一个线性变换.

(ii)设 $X = v_1, \cdots, v_n$ 和 $Y = w_1, \cdots, w_m$ 分别是 V 和 W 的基. 记它们的对偶基分别是 X^* 和 Y^*(见习题 4.35). 若 $S: V \to W$ 是一个线性变换，试证 S^* 的矩阵是一个转置矩阵：

$$_{X^*}[S^*]_{Y^*} = ({_Y}[S]_X)^{\mathrm{T}}.$$

注 下面是值域在函数的定义中是必要的主要原因. 我们刚刚看到，每一个线性变换 $S: V \to W$ 定义了一个线性变换 $S^*: W^* \to V^*$，其定义域为 W^*. 因此改变 S 的值域就改变了 S^* 的定义域，故 S^* 以一种根本的方式改变了. 我们得出结论，函数的值域应该是函数定义的核心部分.

4.37 (i)设 $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$，定义 $\det(A) = ad - bc$. 给定一个系数在一个域中的一个线性方程组 $Ax = 0$，

$$ax + by = p$$
$$cx + dy = q,$$

试证方程组存在唯一一个解当且仅当 $\det(A) \neq 0$.

(ii)设 V 是一个向量空间，v_1，v_2 是其一个基. 定义 $T: V \to V$ 如下：$T(v_1) = av_1 + bv_2$ 及 $T(v_2) = cv_1 + dv_2$. 试证，T 是一个非奇异的线性变换当且仅当 $\det({_X}[T]_X) \neq 0$.

*4.38 设 U 是向量空间 V 的一个子空间.

(i)试证由 $v \mapsto v + U$ 确定的**自然映射** $\pi: V \to V/U$ 是一个线性变换，其核为 U.(商空间在习题 4.16 中有定义.)

382 (ii)叙述并证明向量空间上的**第一同构定理**.

4.39 设 k 是一个域，$k^\times$ 是 k 的非零元素构成的乘法群. 试证 $\det: \mathrm{GL}(2, k) \to k^\times$ 是一个满的群同态，其核为 $\mathrm{SL}(2, k)$. 由此得出结论 $\mathrm{SL}(2, k) \lhd \mathrm{GL}(2, k)$ 且 $\mathrm{GL}(2, k)/\mathrm{SL}(2, k) \cong k^\times$.

H 4.40 设 V 是域 k 上的一个有限维向量空间，$\mathcal{B}$ 是 V 的所有基构成的族. 试证 $\mathcal{B}$ 是一个传递的 $\mathrm{GL}(V)$-集.

4.41 回忆到，若 U 和 W 是向量空间 V 的子空间，且满足 $U + W = V$ 和 $U \cap W = \{0\}$，则称 U 是 V 的直和项，W 为 U 的补. 在习题 4.20 中我们看到，有限维的向量空间的每个子空间都是一个直和项.

(i)设 $U = \{(a, a): a \in \mathbb{R}\}$. 求 U 在 $\mathbb{R}^2$ 中的所有补.

(ii)若 U 是有限维的向量空间 V 一个子空间，试证 U 的任意两个补是同构的.

*4.42 若 A 是一个 $m \times n$ 的矩阵，B 是一个 $p \times m$ 的矩阵，试证

$$\mathrm{rank}(BA) \leqslant \mathrm{rank}(A).$$

4.43 设 $\mathbb{R}^n$ 具有通常的内积：若 $v = (a_1, \cdots, a_n)$，$u = (b_1, \cdots, b_n)$，则 $(v, u) = a_1b_1 + \cdots + a_nb_n$.

(i)线性变换 $U: \mathbb{R}^n \to \mathbb{R}^n$ 称是**正交的**若对所有的 $v, w \in \mathbb{R}^n$，$(Uv, Uw) = (v, w)$.

试证，每一个正交的线性变换都是非奇异的.

(ii)k^n 的**正交基**是满足下性质的基 $v_1, \cdots, v_n$

$$(v_i, v_j) = \delta_{ij},$$

其中(v_i, v_j)是内积，δ_{ij}是克罗内克δ函数. 例如，对通常的内积，标准基就是一个正交基.

试证，一个线性变换$U: \mathbb{R}^n \to \mathbb{R}^n$是正交的当且仅当$U(v_1)$，…，$U(v_n)$是一个正交基若$v_1$，…，$v_n$是一个正交基.

(iii)若$w \in \mathbb{R}^n$，v_1、…，v_n是一个正交基，则$w = \sum_{i=1}^{n} c_i u_i$，试证$c_i = (w, v_i)$.

4.44 设$U: \mathbb{R}^n \to \mathbb{R}^n$是一个正交的线性变换，$X = v_1$，…，$v_n$是一个正交基. 若$O = {}_X[U]_X$，试证$O^{-1} = O^T$. (矩阵$O$称为一个**正交矩阵**).

4.45 设A是一个$n \times n$的实对称矩阵.

(i)举一个非奇异的矩阵的P例子，使得PAP^{-1}是非对称的.

(ii)试证OAO^{-1}是对称的，对每一个实正交矩阵O.

→4.4 特征值

我们来引入方阵的行列式，并用它们来研究矩阵的可逆性. 此节中几个重要的结论将直接给出而不给出证明. 383

一个$n \times n$的实矩阵$A = [a_{ij}]$的行列式通常的定义，尽管它不优美，为：

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n}.$$

回忆到$\operatorname{sgn}(\sigma) = \pm 1$：若$\sigma$是偶置换，则它取$+1$；若$\sigma$是奇置换，则它取$-1$. 项$a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n}$只有一个因子来自$A$的每一行，因为所有第一个下标都是不同的；也只有一个因子来自A的每一列因为所有第二个下标也是不同的. 我们经常称此公式是行列式的**完全展开式**. 由此定义我们看到，$\det(A)$的公式对元素在交换环R中的$n \times n$的矩阵A是有意义的.

考虑行列式的另一个方式是将之看成一个函数

$$D = D_n : \operatorname{Mat}_n(R) \to R.$$

公理化一些合乎需要的D的性质后，人们证明这些性质刻化了D. 接着人们证明这样的函数D存在. 视一个$n \times n$的矩阵$A = [a_{ij}]$不是由n^2个元素，而是由它的行构成的表α_1，…，α_n，其中$\alpha_i = (a_{i1}, \cdots, a_{in}) \in R^n$. 因此$D: R^n \times \cdots \times R^n \to R$，其中有$n$个$R^n$因子. 给定任一个$n$元变量的函数，通过固定其中每组$n-1$个变量，我们可以构造$n$个一元变量的函数. 更详细地，对每个$i$，给定$\alpha_1$，…，$\alpha_n$. 存在函数$d_i: R^n \to R$，其定义如下：

$$d_i(\beta) = D(\alpha_1, \cdots, \alpha_{i-1}, \beta, \alpha_{i+1}, \cdots, \alpha_n).$$

当然，此记号太简化了，它依赖于D和其余行构成的表α_1，…，$\hat{\alpha}_i$，…，α_n.

→ **定义** 设R是一个交换环，视元素在R中的$n \times n$矩阵A为它的行构成表：$A = (\alpha_1, \cdots, \alpha_n)$. 一个$n \times n$的**行列式函数**是一个满足下性质的函数$D: \operatorname{Mat}_n(R) \to R$：

(i)D是**交替的**：若A的两行相等，则$D(A) = 0$，也就是若$\alpha_i = \alpha_j$，$i \neq j$，则$D(\alpha_1, \cdots, \alpha_n) = 0$.

(ii)D是**多重线性的**：对每一个表α_1，…，α_n，由$d_i(\beta) = D(\alpha_1, \cdots, \alpha_{i-1}, \beta, \alpha_{i+1}, \cdots, \alpha_n)$给出的函数$d_i: R^n \to R$满足

$$d_i(\beta + \gamma) = d_i(\beta) + d_i(\gamma), \quad d_i(c\beta) = c d_i(\beta).$$

对所有 $c\in R$ 和所有 $\beta, \gamma\in R^n$；

384 (iii) $D(e_1, \cdots, e_n)=1$，其中 $e_1, \cdots, e_n$ 是标准基，也就是若 I 是单位矩阵，则 $D(I)=1$.

可以证明，对任一个行列式函数 D，有

$$D(AB) = D(A)D(B) \tag{1}$$

和

$$D(A^{\mathrm{T}}) = D(A), \tag{2}$$

其中 A^{T} 是 A 的转置矩阵. 进一步可以证明，$D(A)$ 一定等于完全展开式，因此若 D 存在则它是唯一的. 更准确地，对每一个 $n\geqslant 1$，存在至多一个行列式函数 D：$\mathrm{Mat}_n(R)\to R$.

试图去证明由完全展开式定义的函数 D：$\mathrm{Mat}_n(R)\to R$ 是一个行列式函数看起来是毫无希望的. 我们不是那样做，而是对 $n\geqslant 1$ 进行归纳来证明行列式函数的存在性. 若 $A=[a_{11}]$ 是一个 1×1 的矩阵，定义 $\det(A)=a_{11}$. 对于归纳步，假设存在一个定义在 R 上所有 $(n-1)\times(n-1)$ 的矩阵上的行列式函数 det(必然唯一). 对任意固定的 i，定义

$$D_i^n(A) = \sum_j (-1)^{i+j} a_{ij} \det(A_{ij}), \tag{3}$$

其中 A_{ij} 表示划去 A 的第 i 行和第 j 列而得的 $(n-1)\times(n-1)$ 的矩阵.

→ **定义** 公式(3)称为 $\det(A)$ 在第 i 行的**拉普拉斯展开式**.

对每个 i，D_i^n 是一个行列式函数的证明相当长(例如，参阅科提斯(Curtis)的《线性代数》(Linear Algebra). 此书考虑的是 R 为域这一特殊情形. 至于任意交换环情形的证明是完全不同的，其中应用了“外代数”的理论，请参阅本人的书《高等近世代数》[⊖]). 因为对每一个 i，在第 i 行的拉普拉斯(Laplace)展开式是一个行列式函数，由行列式函数的唯一性可推出行列式可应用在任一行的拉普拉斯展开式的计算. 进一步，由于方程(2)可写成 $\det(A^{\mathrm{T}})=\det(A)$，由此推出 $\det(A)$ 可通过任一列的拉普拉斯展开式来计算(因为转置将行，列对换了). 拉普拉斯展开式，最关键的优点是适用于归纳证明. 例如，应用归纳法是求解习题 4.51 的最容易的方法：若 A 是一个三角矩阵，则 $\det(A)$ 是它的对角线上元素的积.

当 k 是一个域时，有一个计算 $\det(A)$ 有效的方法，应用初等变换 $A\to A'$，将矩阵 A 变成矩阵 A'：

类型Ⅰ 将 A 的某一行的某纯量倍加至另一行；

类型Ⅱ 用某非零 $c\in k$ 乘以 A 的某一行；

385 **类型Ⅲ** 对换 A 的两行.

若 $A\to A'$ 是一个初等行变换，则对某 $r\in k$ $\det(A')=r\det(A)$. 若此变换是类型Ⅱ的，则行列式函数的多重线性表明 $r=c$；对于类型Ⅰ的初等变换，习题 4.47 表明 $r=1$；对于类型Ⅲ的初等变换，习题 4.49 表明 $r=-1$. 当 k 是一个域时，习题 4.26 说由高斯消元法我们可以将 A 化成三角形矩阵：存在一系列的初等行变换

$$A \to A_1 \to A_2 \to \cdots \to A_q = \triangle,$$

其中 $\triangle$ 是三角形矩阵. 因此，我们可用 $\det(\triangle)$ 和这一串变换来计算 $\det(A)$，而习题 4.15 表

⊖ 本书中文版已由机械工业出版社出版——编辑注.

明，det(△)是它的主对角线上的元素的乘积.

让我们回到元素在任一个交换环 R 中的矩阵. 现在我们修改类型Ⅱ的初等变换的定义为：用一个单位 $c\in R$ 去乘 A 的某一行.

→ **定义** 交换环 R 上的一个 $n\times n$ 矩阵 A 是**可逆的**若存在一个(元素在 R 中)满足 $AB=I=BA$ 的矩阵 B.

当 R 是一个域时，可逆的称为非奇异的. 推论 4.88 表明交换环 R 上的矩阵是可逆的当且仅当它的行列式是 R 中的一个单位.

→ **定义** 设 $A=[a_{ij}]$ 是交换环 R 上的一个 $n\times n$ 矩阵. A 的**伴随**[⊖]是指下面的矩阵

$$\operatorname{adj}(A)=[c_{ij}],$$

其中

$$c_{ji}=(-1)^{i+j}\det(A_{ij}),$$

A_{ij} 表示在 A 中划去它的第 i 行和第 j 列后而得的 $(n-1)\times(n-1)$ 的矩阵.

下标反过来是故意的. 总之，$\operatorname{adj}(A)$ 是 ij 位元素是 $(-1)^{i+j}\det(A_{ij})$ 的矩阵的转置. 我们经常称为 c_{ij} 为 A 的 ij-**余子式**.

例如，若

$$A=\begin{bmatrix}a & b\\ c & d\end{bmatrix},$$

则

$$\operatorname{adj}(A)=\begin{bmatrix}d & -c\\ -b & a\end{bmatrix}^{\mathrm{T}}=\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}.$$ 386

→ **命题 4.87** 若 A 是交换环 R 上的一个 $n\times n$ 的矩阵，则

$$A\operatorname{adj}(A)=\det(A)I=\operatorname{adj}(A)A.$$

证明 设 $A=[a_{ij}]$，在此证明中，记 a_{ij} 为 $(A)_{ij}$. 因此若 $C=[c_{ij}]$，则 $(AC)_{ii}=\sum_k a_{ik}c_{kj}$. 若我们定义 $C=[c_{ij}]$：$c_{ij}=(-1)^{i+j}\det(A_{ji})$[这样 $C=\operatorname{adj}(A)$]，则由 A 的第 i 行的拉普拉斯展开式可得

$$(AC)_{ii}=\sum_k(-1)^{i+k}a_{ik}\det(A_{ik})=\det(A).$$

在计算 $(AC)_{ij}$ 之前我们先停顿一下，这里 $j\neq i$. 定义 $M=[m_{pq}]$ 为将 A 的第 j 行 $(a_{j1},\cdots,a_{jn})$ 替换为第 i 行 $(a_{i1},\cdots,a_{in})$ 后而得的矩阵. 因此对所有 k 有 $m_{jk}=a_{ik}$. 注意，对所有的 k 有 $M_{jk}=A_{jk}$(因为 M 和 A 只是在第 j 列不同，而在获得更小的矩阵 M_{jk} 和 A_{jk} 时，此行被划去了).

当 $j\neq i$ 时，

$$\begin{aligned}(AC)_{ij}&=\sum_k a_{ik}(-1)^{i+k}\det(A_{jk})\\&=\sum_k(-1)^{i+k}m_{jk}\det(M_{jk})\\&=\det(M),\end{aligned}$$

⊖ 4.3 节中有另一个伴随的概念，与此无联系.

因为 $a_{ik}=m_{jk}$ 且 $M_{jk}=A_{jk}$. 但 $\det(M)=0$，因为它有两行相等. 因此，$A\,\mathrm{adj}(A)=AC$ 是一个纯量矩阵，其对角线上元素全等于 $\det(A)$. ■

→ **推论 4.88** 若 A 是元素在交换环 R 中的一个 $n\times n$ 矩阵，则 A 是可逆的当且仅当 $\det(A)$ 是 R 中的一个单位. 进一步，

$$\det(A^{-1})=\det(A)^{-1}.$$

证明 若 A 是可逆的，则存在一个矩阵 B 使得 $AB=I$. 由(1)可知，$1=\det(I)=\det(AB)=\det(A)\det(B)$，所以 $\det(A)$ 是 R 中的一个单位. 反之，假设 $\det(A)$ 是 R 中的一个单位. 若 $B=\det(A)^{-1}\mathrm{adj}(A)$，则由命题 4.87，知 $AB=I=BA$.

而 $I=AA^{-1}$ 给出 $1=\det(I)=\det(AA^{-1})=\det(A)\det(A^{-1})$. 因此 $\det(A^{-1})=\det(A)^{-1}$. ■

在 R 是域这个特殊情形中，我们看到 A 是可逆的(即 A 是非奇异的)当且仅当 $\det(A)\neq 0$. (这是来自标准线性代数课程中的一个熟知的结论). 另一方面，若 A 是一个元素在$\mathbb{Z}$中的 $n\times n$ 的矩阵，则 A 是可逆的当且仅当 $\det(A)=\pm 1$，也就是，A^{-1} 存在且其元素为整数当且仅当
387 $\det(A)=\pm 1$. 若 $R=k[x]$，其中 k 是域，则 A 是可逆的当且仅当它的行列式是非零常数.

推论 4.89 设 P 和 M 是元素在交换环 R 中的 $n\times n$ 的矩阵. 若 P 是可逆的，则

$$\det(PMP^{-1})=\det(M).$$

证明 由推论 4.88 知，我们有 $\det(P^{-1})=\det(P)^{-1}$. 因为行列式在交换环 R 中，所以.

$$\begin{aligned}\det(PMP^{-1})&=\det(P)\det(M)\det(P^{-1})\\&=\det(M)\det(P)\det(P^{-1})=\det(M).\end{aligned}$$ ■

推论 4.90 设 $T:V\to V$ 为域 k 上向量空间 V 上的一个线性变换，且 X 和 Y 为 V 的基. 若 $A={}_X[T]_X$ 和 $B={}_Y[T]_Y$，则 $\det(A)=\det(B)$.

证明 由推论 4.74，A 和 B 是相似的；也就是存在一个非奇异的(因此可逆的)矩阵 P，使得 $B=PAP^{-1}$. ■

由此推论得出，线性变换 T 的(在不同基上)矩阵有相同的行列式，因此我们现在可以定义线性变换的行列式.

→ **定义** 若 $T:V\to V$ 是有限维向量空间 V 上的一个线性变换，则

$$\det(T)=\det(A),$$

其中对 V 的某个基 X，$A={}_X[T]_X$.

像我们刚刚提及的一样，此定义不依赖于 X 选择.

也许最简单的线性变换 $T:V\to V$ 就是纯量变换 $T=c1_V$；也就是，存在一个纯量 $c\in k$ 使得 $T(v)=cv$，对所有的 $v\in V$. 我们现在问，对任意一个线性变换 $T:V\to V$，是否存在 $c\in k$ 使得 $T(v)=cv$，对某些 $v\in V$(当然，只有 $v\neq 0$ 时才有趣).

→ **定义** 设 $T:V\to V$ 是一个线性变换，其中 V 是域 k 一个有限维向量空间. 一个纯量 $c\in k$ 称为 T 的特征值[⊖]，若存在满足

⊖ 原文为"eigenvalue"，部分译自德文单词"Eigenwert"("Wert"意思为数值)，"eigen"的意思是"特殊的"或"合适的". 故经常用 characteristic value 代替 eigenvalue. 这种部分译翻译法在其他单词中也有应用(例如，德文单词 Eigenvecktor 就被译成 eigenvector 和 characteristic vector).

$$T(v) = cv.$$ 388

的非零向量 v，称 v 为 T 的特征向量.

命题 4.91 设 $T: V \to V$ 是一个线性变换，其中 V 是域 k 上的一个向量空间. 再设 c_1，c_2，…，c_r 为 T 在 k 中的特征值. 若 v_i 为 T 的属于 c_i 的特征向量，则表 $X = v_1$，…，v_r 是线性无关的.

证明 对 $r \geqslant 1$ 用归纳法. 基础步骤 $r=1$ 成立，因为任意一非零向量是一个长度为 1 的线性无关的表，而由定义，特征向量是非零的. 下面证明归纳步，假设

$$a_1 v_1 + \cdots + a_{r+1} v_{r+1} = 0.$$

用 T 作用此等式，则有

$$a_1 c_1 v_1 + \cdots + a_{r+1} c_{r+1} v_{r+1} = 0.$$

用 c_{r+1}乘第一个方程，再用第二方程减之，则有

$$a_1(c_1 - c_{r+1})v_1 + \cdots + a_r(c_r - c_{r+1})v_r = 0.$$

由归纳假设，对所有 $i \leqslant r$，$a_i(c_i - c_{r+1}) = 0$. 因为所有特征值是不同的，故 $c_i - c_{r+1} \neq 0$，所以 $a_i = 0$，对所有 $i \leqslant r$. 原始的等式就变成了 $a_{r+1} v_{r+1} = 0$，故由基础步骤，$a_{r+1} = 0$，所以所有系数 a_i 是零，从而 v_1，…，v_{r+1}是线性无关的. ■

引理 4.92 设 $T: V \to V$ 是域 k 上一个向量空间 V 上的一个线性变换，则 $c \in k$ 是 T 的一个特征值当且仅当 $c1_V - T$ 是奇异的.

证明 若 c 是 T 的一个特征值，则存在一个非零向量 $v \in V$ 满足 $T(v) = cv$，因此 $(c1_V - T)(v) = 0$，从而 $c1_V - T$ 是奇异的. 反之，若 $c1_V - T$ 是奇异的，则推论 4.81 提供了一个满足 $(c1_V - T)(v) = 0$ 的非零向量 v. 因此 $T(v) = cv$，且 c 为 T 的一个特征值. ■

我们已经被引导至考虑形如 $cI - T$ 的线性变换，对某纯量 $c \in k$. 这引导我们去考虑矩阵 $xI - A$，其中 A 是表示 T 的一个矩阵，因为我们研究了元素在交换环中的矩阵，因此我们计算 $xI - A$ 这个元素属于 $k[x]$的矩阵的行列式是有理论根据的.

→ **定义** 若 A 是元素在域 k 上的一个 $n \times n$ 的矩阵，则它的**特征多项式**[⊖]为 $h_A(x) = \det(xI - A)$.

若 $T: V \to V$ 是 n 维向量空间 V 上的一个线性变换，则**特征多项式** $h_T(x)$定义为 $h_A(x)$，其中 $A = {}_X[T]_X$ 是任一个表示 T 的矩阵. 389

若 R 是一个交换环，A 是元素在 R 中的一个 $n \times n$ 的矩阵，则 $\det(A) \in R$. 特别地，$xI - A$ 的元素在 $R = k[x]$中，其中 k 是一个域，所以 $h_A(x) = \det(xI - A) \in k[x]$，也就是说，特征多项式确实是一个多项式.

下一个命题通过证明 $\det(xI - A)$不依赖于表示 T 的矩阵 A 的选择来表明 $h_T(x) = \det(xI - A)$是定义良好的.

命题 4.93 若 A 和 B 是元素在域 k 上的两个相似的 $n \times n$ 的矩阵，则它们有相同的特征多

⊖ 没有人称 characteristic polynomial 为 eigenpolynomial.

项式：

$$h_A(x)=\det(xI-A)=\det(xI-B)=h_B(x).$$

证明 若 $B=PAP^{-1}$，则

$$P(xI-A)P^{-1}=PxIP^{-1}-PAP^{-1}=xI-B.$$

因此 $\det(P(xI-A)P^{-1})=\det(xI-B)$. 但

$$\det(P(xI-A)P^{-1})=\det(P)\det(xI-A)\det(P^{-1})=\det(xI-A).$$ ■

推论 4.94 (i)设 A 是域 k 上的一个 $n\times n$ 的矩阵. 若它的特征多项式 $h_A(x)$ 在 k 上分裂，则纯量 $c\in k$ 是 A 的一个特征值当且仅当 c 为 $h_A(x)$ 的一个根.

(ii)相似的矩阵有相同的特征值，且特征值出现的重数也相同.

证明 (i)由推论 4.88，$cI-A$ 是奇异的当且仅当 $h_A(c)=\det(cI-A)=0$. 因此由引理 4.92，c 是一个特征值当且仅当 c 是特征多项式的根.

(ii)由命题 4.93，A 和 B 有相同的特征多项式. 由(i)知，A 和 B 有相同的特征值，且出现的重数也一样. ■

矩阵 A 的每一个特征值都是 $h_A(x)$ 的一个根，但特征多项式也许有根不在 k 中. 例如，视 $A=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ 为$\mathbb{R}$上的一个矩阵，其特征多项式为 x^2+1，它的根为$\pm$i. 因为这些根不在$\mathbb{R}$中，所以它们中的任一个均无$\mathbb{R}^2$ 中的特征向量，即不存在实数 a 和 b 使得 $\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}=\begin{bmatrix}ia\\ ib\end{bmatrix}$. 然而，如果我们将 A 视为一个复矩阵(它的元素碰巧为实数)，则我们能出求特征向量. 例如，$(1, i)^T$ 就为一个特征向量. 几乎所有的人将特征值的定义拓展以使得特征值包括这样
390 的根(当然，如果 $h_A(x)$ 的所有根都在 k 中，则没有新的特征值会出现).

→ **注** 下面的“技巧”可使得我们免除推论 4.94 中的假设：特征多项式在 k 上分裂. 设 A 为域 k 上的一个 $n\times n$ 的矩阵，设 $T: k^n\to k^n$ 为满足 $T(x)=Ax$ 的线性变换，其中 $x\in k^n$ 是一个列向量，由克罗内克定理(定理 3.18)，存在扩域 K/k，它包含了 $h_A(x)$ 的所有根：也就是 K 包含 A 的所有特征值. 定义线性变换 $\widetilde{T}: K^n\to K^n$ 为 $\widetilde{T}(\tilde{x})=A\tilde{x}$，其中 $\tilde{x}\in K^n$ 是一个列向量. 由我们原来对特征值的讨论可知，若 $c\in K$ 是 A 的一个特征值，则存在一个特征向量 $\tilde{v}\in K^n$ 满足 $\widetilde{T}(\tilde{v})=c\tilde{v}$.

→ **定义** 若 $A=[a_{ij}]$ 是一个 $n\times n$ 的矩阵，则它的迹为它的对角线上元素的和：

$$\operatorname{tr}(A)=\sum_{i=1}^{n}a_{ii}.$$

命题 4.95 设 k 是一个域，A 为元素在 k 中的一个 $n\times n$ 的矩阵，则 $h_A(x)$ 是一个次数为 n 的首一多项式. 进一步，$h_A(x)$ 中 x^{n-1} 的系数为 $-\operatorname{tr}(A)$ 且常数项为 $(-1)^n\det(A)$.

证明 设 $A=[a_{ij}]$，$B=xI-A$. 则 $B=[b_{ij}]=[x\delta_{ij}-a_{ij}]$，其中 δ_{ij} 是克罗内克 δ 函数，其完全展开式是

$$\det(B)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)b_{\sigma(1),1}b_{\sigma(2),2}\cdots b_{\sigma(n),n}.$$

若 σ 是恒等元(1)，则它对应的 $\det(B)=\det(xI-A)$ 的完全展开式中的项为

$$b_{11}\cdots b_{nn}=(x-a_{11})(x-a_{22})\cdots(x-a_{nn})=\prod_i(x-a_{ii}),$$

它是 $k[x]$ 中一个次数为 n 的首一多项式. 若 $\sigma\neq(1)$，则完全展开式中 σ 对应的项不可能恰好有 $n-1$ 个因子在 $xI-A$ 的对角线中，因为若 σ 固定 $n-1$ 个数码，则 $\sigma=(1)$. 因此 $\sigma\neq(1)$ 的所有对应的项的和或者为 0 或者是 $k[x]$ 中次数至多为 $n-2$ 的多项式. 因此 $\deg(h_A)=n$. 由习题 3.102 知，x^{n-1} 的系数是 $-\sum_i a_{ii}=-\mathrm{tr}(A)$，$h_A(x)$ 的常数项为 $h_A(0)=\det(-A)=(-1)^n\det(A)$. ■

推论 4.96 *若 A 和 B 是元素在域 k 中的相似矩阵，则 A，B 具有相同的迹和行列式.*

证明 由命题 4.93，A 和 B 有相同的特征多项式，应用命题 4.95 即给出 $\mathrm{tr}(A)=\mathrm{tr}(B)$ 且 $\det(A)=\det(B)$. ■

设 A 和 B 是相似矩阵. $\mathrm{tr}(A)=\mathrm{tr}(B)$ 的另一个证明在习题 4.56 中有所描述，而推论 4.89 表明了 $\det(A)=\det(B)$. 391

推论 4.97 *若 $T: V\to V$ 是一个线性变换，$\dim(V)=n$，则 T 至多有 n 个特征值.*

证明 若 $\dim(V)=n$，则由命题 4.95 知 $\deg(h_T)=n$. 所以由定理 3.50 知结论成立. ■

下面的推论阐明了迹的特征值的和(重根按重数计)且行列式是特征值的积(重根按重数计).

推论 4.98 *设 $A=[a_{ij}]$ 为元素在域 k 中的一个 $n\times n$ 的矩阵，且设 $h_A(x)=\prod_{i=1}^n(x-\alpha_i)$ 为它的特征多项式，则*

$$\mathrm{tr}(A)=\sum_i\alpha_i,\quad \det(A)=\prod_i\alpha_i.$$

证明 由习题 3.102 知，若 $f(x)=\sum_j c_jx^j\in k[x]$ 是一个首一多项式，且 $f(x)=\prod_{i=1}^n(x-\alpha_i)$，则 $c_{n-1}=-\sum_j\alpha_j$ 且 $c_0=(-1)^n\prod_j\alpha_j$. 特别地，当 $f(x)=h_A(x)$ 时也成立. 这样由命题 4.95 知结论成立，因为命题 4.95 指出 c_{n-1} 等于 $-\mathrm{tr}(A)$，而 c_0 等于 $(-1)^n\det(A)$(在每一种情形下，符号都可以去掉).

例 4.99 视 $A=\begin{bmatrix}1&2\\3&4\end{bmatrix}$ 为 $\mathrm{Mat}_2(\mathbb{Q})$ 中的一个矩阵. 它的特征多项式是

$$h_A(x)=\det\left(\begin{bmatrix}x-1&-2\\-3&x-4\end{bmatrix}\right)=x^2-5x-2.$$

由二次求根公式可求出 A 的特征值为 $\frac{1}{2}(5\pm\sqrt{33})$. 注意

$$-\mathrm{tr}(A)=-\frac{1}{2}(5+\sqrt{33})+\frac{1}{2}(5-\sqrt{33})=5;$$

$$\det(A)=\frac{1}{2}(5+\sqrt{33})\,\frac{1}{2}(5-\sqrt{33})=-2$$ ◀

若纯量矩阵是最简单的矩阵，则对角矩阵是第二简单的，这里 $n\times n$ 的矩阵 $D=[d_{ij}]$是**对角矩阵**若对所有 $i\neq j$ 它的所有对角线外的元素 $d_{ij}=0$.

→ **定义** 一个 $n\times n$ 的矩阵 A 称为是**可对角化的**，若 A 相似于一个对角矩阵.

392 当然，每一个对角线矩阵是可对角化的.

命题 4.100 (i)域 k 上一个 $n\times n$ 的矩阵是可对角化的当且仅当 k^n 存在一组由 A 的特征向量组成的基.

(ii)若 A 相似于一个对角形矩阵 D，则 D 的对角线上的元素就是 A 的特征值(具有相同重数).

证明 (i)与通常情况一样，定义线性变换 $T: k^n\to k^n$ 为 $T(v)=Av$. 若 A 相似于一个对角矩阵$D=[d_{ij}]$,则存在 k^n 的一组基 $X=v_1, \cdots, v_n$ 使得 $D={}_X[T]_X$，也就是 $T(v_j)=d_{1j}v_1+\cdots+d_{nj}v_n$. 因为 D 是对角形，我们有 $T(v_j)=d_{jj}v_j$，所以 X 由特征向量组成(所有 v_j 是非零的，因为 0 永远不会是基的一部分)

相反地，设 $X=v_1, \cdots, v_n$ 为 k^n 的由特征向量组成的一组基，如对所有 j 设 $T(v_j)=c_jv_j$ 对所有的 j，$B={}_X[T]_X$ 的第 j 列为$[0, \cdots, 0, c_j, 0, \cdots, 0]^T$. 因此 B 是一个对角形矩阵，且对角线上元素为 $c_1, \cdots, c_n$. 最后，A 和 B 是相似的，因为它们是线性变换 T 在不同的基中的表示.

(ii) 若 D 是一个对角矩阵，对角线上元素为 d_{ii}，则 $\det(xI-D)=\prod_i(x-d_{ii})$. 因此 D 的特征值为它的对角线上元素. 因为 A 和 B 是相似的，命题 4.39 表明它们有相同的特征值(具有相同的重数). ■

例 4.101 下面是一个不可对角化的 2×2 的矩阵的例子. 若 $A=\begin{bmatrix}1&1\\0&1\end{bmatrix}$，则它只有一个特征值，即 1(重数为 2). 由命题 4.100(ii)可知，若 A 相似于一个对角形矩阵 D，则 $D=\begin{bmatrix}1&0\\0&1\end{bmatrix}=I$，从而 $A=PIP^{-1}=I$，矛盾. ◀

→ **推论 4.102** 设 A 是域 k 上的一个 $n\times n$ 的矩阵，k 包含 A 的所有特征值. 若 A 的特征多项式无重根，则 A 可对角化.

注 回忆习题 3.67：多项式 $f(x)\in k[x]$无重根当且仅当 $\gcd(f, f')=1$，其中 $f'(x)$ 是 $f(x)$的导数.

证明 因为 $\deg(h_A)=n$，所以 A 有 n 个不同的特征值 $c_1, \cdots, c_n$. 因为这些特征值均在 k 中，故 k^n 中的有相应的特征向量 $v_1, \cdots, v_n$，也就是 $Av_i=c_iv_i$. 由命题 4.91，表 $v_1, \cdots, v_n$ 是线性无关的，因此它为 k^n 的一组基. 由命题 4.100 可知结论成立. ■

推论 4.102 的逆命题是不成立的. 例如，2×2 的单位矩阵 I 显然是可对角化的(它实际上
393 是对角形)，然而它的特征多项式 x^2-2x+1 有重根.

例 4.103 设 $A=\begin{bmatrix}a&b\\b&c\end{bmatrix}$为一个实(对称)矩阵. 我们断言 A 的特征值是实的. $h_A(x)=x^2-$

$(a+c)x+(ac-b^2)$. 由二次求根公式可得特征值为

$$x=\frac{1}{2}[(a+c)\pm\sqrt{(a+c)^2-4(ac-b^2)}].$$

但$(a+c)^2-4(ac-b^2)=(a-c)^2+4b^2\geqslant 0$. 因此它的平方根是实的，从而特征值 x 是实的. ◀

如何来推广例 4.103 中的论断至 $n\geqslant 3$ 情形是不明显的，但结论是对的：实对称矩阵的特征值是实的. 此结果称为*主轴定理*，因为它可应用于求(高维)圆锥曲线的规范形.

回忆例 4.67：若 $T:\mathbb{R}^n\to\mathbb{R}^n$ 是一个线性变换，则它的伴随是线性变换 $T^*:\mathbb{R}^n\to\mathbb{R}^n$，且对所有 u，$v\in\mathbb{R}^n$ 满足

$$(Tu,v)=(u,T^*v),$$

其中(u, v)是通常的内积. 此例也表明，若 $A={}_E[T]_E$，则${}_E[T^*]_E=A^T$. 因此若 A 是一个对称矩阵，则 $T=T^*$.

因为实矩阵的特征值可以为复数，所以我们从将$\mathbb{R}^n$ 上的内积推广至$\mathbb{C}^n$ 上的内积开始. 通常的公式$(u, v)=a_1c_1+\cdots+a_nc_n$，其中 $u=(a_1, \cdots, a_n)$，$v=(c_1, \cdots, c_n)$是一个内积，但它是退化的. 例如$\mathbb{C}^n$ 中非零向量 $u=(1, \mathrm{i})$满足$(u, u)=1^2+\mathrm{i}^2=0$.

→ **定义** $\mathbb{C}^n$ 上**埃尔米特(Hermitian)型**定义如下：

$$(u,v)=a_1\bar{c}_1+\cdots+a_n\bar{c}_n,$$

其中 $u=(a_1, \cdots, a_n)$，$v=(c_1, \cdots, c_n)\in\mathbb{C}^n$.

埃尔米特型是非退化的，因为$(u, u)=a_1\bar{a}_1+\cdots+a_n\bar{a}_n$是实平方数的和，所以立即有$(u, u)=0$ 当且仅当 $u=0$. 易证明$(u+u', v)=(u, v)+(u', v)$，其中 u，u'，$v\in\mathbb{C}^n$. 然而，它不是一个内积，因为$(v, u)=(u, v)$不总是成立. 事实上，$(v, u)=c_1\bar{a}_1+\cdots+c_n\bar{a}_n=\overline{(u, v)}$. 因此$(u, qv)=\overline{(qv, u)}=\overline{q(v, u)}=\bar{q}\overline{(v, u)}=\bar{q}(u, v)$. 从而，对所有 $q\in\mathbb{C}$，

$$(u,qv)=\bar{q}(u,v).$$

→ **定理 4.104(主轴定理)** *若 A 是一个 $n\times n$ 的实对称矩阵，则它的所有特征值是实的且 A 是可对角化的.* 394

证明 设$(,)$为$\mathbb{C}^n$上的埃尔米特型，习题 4.54 表明若 T：$\mathbb{C}^n\to\mathbb{C}^n$ 是一个线性变换，则存在一个线性变换 $T^\#:\mathbb{C}^n\to\mathbb{C}^n$ 使得$(Tu, v)=(u, T^\# v)$. 特别地，矩阵乘法 $v\mapsto Av$ 确定了一个线性变换 $T:\mathbb{C}^n\to\mathbb{C}^n$. 习题 4.54 也表明了若 A 是一个实对称矩阵，则 $T^\#=T$；也就是对所有 u，$v\in\mathbb{C}^n$，

$$(Tu,v)=(u,Tv).$$

现在我们能够通过证明 T(和 A)的所有特征值是实的来推广例 4.103. 若 $c\in\mathbb{C}$ 是 T 的一个特征值(它是存在的，因为$\mathbb{C}$ 是代数封闭的)，则存在一个非零 $v\in\mathbb{C}^n$ 满足 $T(v)=cv$. 我们用两种方式来计算(Tv, v)的值. 一方面，$(Tv, v)=(cv, v)=c(v, v)$，另一方面，因为 $T=T^\#$，我们有$(Tv, v)=(v, Tv)=(v, cv)=\bar{c}(v, v)$. 而$(v, v)\neq 0$ 因为 $v\neq 0$. 故 $c=\bar{c}$，也就是 c 为实的.

我们在通过对 $n\geqslant 1$ 进行归纳来证明 A 是可对角化的. 因为基础步骤 $n=1$ 是显然成立的，故

我们进入归纳步. 取 A 的一个特征值 c. 因为 c 是实的，所以存在特征向量 $v\in\mathbb{R}^n$ 满足 $Av=cv$. 注意由习题 4.21 可知，$\mathbb{R}^n=\langle v\rangle\oplus\langle v\rangle^{\perp}$，所以 $\dim(\langle v\rangle^{\perp})=n-1$. 我们断言 $T(\langle v\rangle^{\perp})\subseteq\langle v\rangle^{\perp}$. 若 $w\in\langle v\rangle^{\perp}$，则 $(w, v)=0$. 我们必须证明 $(Tw, v)=0$. 因为 A 是对称的，于是 $(Tw, v)=(w, T^{\#}v)=(w, Tv)$. 但 $(w, Tv)=(w, cv)=\bar{c}(w, v)=0$，所以 $T(w)\in\langle v\rangle^{\perp}$，得证. 若 T' 是 T 在 $\langle v\rangle^{\perp}$ 上的限制，则 $T':\langle v\rangle^{\perp}\to\langle v\rangle^{\perp}$. 因为对所有 $u, w\in\mathbb{R}^n$ 都有 $(Tu, w)=(u, Tw)$. 所以特别地，对所有 $u, w\in\langle v\rangle^{\perp}$，我们有 $(T'u, w)=(u, T'w)$. 因此，应用归纳假设，T' 是可对角化的. 命题 4.100 说，存在一组由 T' 的从而也是 T 的特征向量组成的 $\langle v\rangle^{\perp}$ 的基 $v_2, \cdots, v_n$，而 $v, v_2, \cdots, v_n$ 是 $\mathbb{R}^n=\langle v\rangle\oplus\langle v\rangle^{\perp}$ 的一组基，因此 A 是可对角化的(再一次应用命题 4.100). ■

为了理解为什么有些矩阵不是可对角化的，最好考虑更一般的问题：两个任意的 $n\times n$ 的矩阵何时是相似的. 给定域 k 上一个矩阵 A，基本的想法是找一个相似于 A 的“最简单的”矩阵 C. 这样的矩阵 C 称为 A 的标准型. 标准型第一个可能的候选是对角形矩阵，但例 4.101 说这还不够. 可以证明，每一个矩阵有两个常用的标准形：**有理标准形和约当(Jordan)标准形**. 这些标准形的每一个都是为特殊的应用而设置的. 例如，有理标准形的元素总是落在域 k 上的(然而，A 的所有特征值都作为约当标准形的元素出现)，这结果在证明下面的结论时有需要.

→ **定理** *设 A 和 B 为域 k 上的 $n\times n$ 的矩阵. K/k 是一个域扩张. 若 A 和 B 在 K 上相似，则它们在 k 上也相似. 也就是，若存在 K 上一个非奇异矩阵 P 使得 $PAP^{-1}=B$，则存在 k 上*
395 *一个非奇异矩阵 Q 使得 $QAQ^{-1}=B$.*

例如，两个在 $\mathbb{C}$ 上相似的实矩阵在 $\mathbb{R}$ 上也相似. 两个标准形都可应用至证明下面的定理：每一个 $n\times n$ 的矩阵均相似于它的转置.

可以证明，有理标准型的方幂是复杂的，而约当标准形的方幂很容易计算. 很明显地，约当标准形的性质被应用于求一个非奇异矩阵在一般线性群中的阶. 此性质也用于证明凯莱-哈密顿(Cayley-Hamilton)定理

→ **定理(凯莱-哈密顿)** *设 A 为一个 $n\times n$ 的矩阵，其特征多项式为 $h_A(x)=c_0+c_1x+c_2x^2+\cdots+x^n$. 则*

$$c_0I+c_1A+c_2A^2+\cdots+A^n=0.$$

也存在不用标准形的凯莱-哈密顿定理的证明. (例如，见贝克霍夫-麦克伦(Birkhoff-MacLane)的书).

习题

H 4.46 判断正误并给出理由.

(i)若矩阵 A 相似于一个对称矩阵，则 A 是对称的.

(ii) $\begin{bmatrix}2 & 1\\0 & 1\end{bmatrix}$ 在 $\mathbb{Q}$ 上可逆的.

(iii) $\begin{bmatrix}2 & 1\\0 & 1\end{bmatrix}$ 在 $\mathbb{Z}$ 上是可逆的.

(iv)若 A 是 $\mathbb{R}$ 上一个元素均为正的 2×2 的矩阵，则 $\det(A)$ 是正的.

(v)若 A 是ℝ上一个元素均为正的 2×2 的矩阵，则 $\det(A)\geqslant0$.

(vi)若 A 和 B 是 $n\times n$ 的矩阵，则 $\mathrm{tr}(A+B)=\mathrm{tr}(A)+\mathrm{tr}(B)$.

(vii)若域 k 上两个 $n\times n$ 的矩阵具有相同的特征多项式，则它们是相似的.

(viii)若 $A=\begin{bmatrix}1&2\\3&4\end{bmatrix}$，则 $A^2-5A-2I=0$.

(ix)ℝ上每一个 $n\times n$ 的矩阵有一个实特征值.

(x) $\begin{bmatrix}2&1&7\\0&1&8\\0&0&0\end{bmatrix}$ 是可对角化的.

*4.47 设 R 是一个交换环，$D:\mathrm{Mat}_n(R)\to R$ 是一个行列式函数且 A 是一个 $n\times n$ 的矩阵，其行为 $\alpha_1,\cdots,\alpha_n$. 定义 $d_i:R^n\to R$ 为 $d_i(\beta)=D(\alpha_i,\cdots,\alpha_{i-1},\beta,\alpha_{i+1},\cdots,\alpha_n)$.

(i)若 $i\neq j$，$r\in R$，试证

$$d_i(r\alpha_j)=0.$$

(ii)若 $i\neq j$，$r\in R$，试证 $d_i(\alpha_i+r\alpha_j)=D(A)$.

(iii)若 $r_j\in R$，试证

$$d_i\Big(\alpha_i+\sum_{j\neq i}r_j\alpha_j\Big)=D(A).$$ 396

4.48 若 O 是一个正交矩阵，试证明 $\det(O)=\pm1$.

*H 4.49 若 A' 是对换 $n\times n$ 的矩阵 A 的两行而得的矩阵，试证 $\det(A')=-\det(A)$.

4.50 若 A 是交换环 R 上的一个 $n\times n$ 的矩阵，$r\in R$. 试证 $\det(rA)=r^n\det(A)$. 特别地 $\det(-A)=(-1)^n\det(A)$.

*4.51 若 $A=[a_{ij}]$ 是一个 $n\times n$ 的三角矩阵，试证

$$\det(A)=a_{11}a_{22}\cdots a_{nn}.$$

*4.52 若 $u_1,\cdots,u_n$ 是域 k 中的一个表，则相应的**范德蒙德矩阵**为

$$V=\mathrm{Van}(u_1,\cdots,u_n)=\begin{bmatrix}1&u_1&u_1^2&u_1^3&\cdots&u_1^{n-1}\\1&u_2&u_2^2&u_2^3&\cdots&u_2^{n-1}\\\vdots&\vdots&\cdots&\cdots&\vdots&\vdots\\1&u_n&u_n^2&u_n^3&\cdots&u_n^{n-1}\end{bmatrix}.$$

(i)试证

$$\det(V)=\prod_{i<j}(u_j-u_i).$$

由此得出 V 是非奇异的若所有 u_i 是不同的.

H (ii)若 ω 是一个本原 n 次单位根(对 $i<n$，$\omega^n=1$ 且 $\omega^i\neq1$). 试证 $\mathrm{Van}(1,\omega,\omega^2,\cdots,\omega^{n-1})$ 是非奇异的且

$$\mathrm{Van}(1,\omega,\omega^2,\cdots,\omega^{n-1})^{-1}=\frac{1}{n}\mathrm{Van}(1,\omega^{-1},\omega^{-2},\cdots,\omega^{-n+1}).$$

(iii)设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in k[x]$ 且设 $y_i=f(u_i)$. 试证系数向量 $a=(a_0,a_1,\cdots,a_n)$ 是下面线性方程组的一个解

$$Vx=y \tag{4}$$

其中 $y=(y_0,\cdots,y_n)$. 由此得出若所有 u_i 是不同的，则 $f(x)$ 由(4)决定.

4.53 定义**三对角矩阵**为具有如下形式的一个 $n\times n$ 的矩阵

$$T[x_1,\cdots,x_n]=\begin{bmatrix} x_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ -1 & x_2 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & -1 & x_3 & 1 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & x_4 & \cdots & 0 & 0 & 0 & 0 \\ & & \vdots & & \ddots & & \vdots & & \\ 0 & 0 & 0 & 0 & \cdots & x_{n-3} & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -1 & x_{n-2} & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & x_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & x_n \end{bmatrix}.$$

(i)若 $D_n=\det(T[x_1,\ \cdots,\ x_n])$，试证 $D_1=x_1$，$D_2=x_1x_2+1$ 且对所有 $n>2$，

397 $$D_n = x_nD_{n-1}+D_{n-2}.$$

(ii)证明，若所有 $x_i=1$，则 $D_n=F_{n+1}$，即第 n 项斐波那契数.（回忆到 $F_0=0$，$F_1=1$ 且对所有 $n\geq 2$ $F_n=F_{n-1}+F_{n-2}$.）

*4.54 设 $T:\mathbb{C}^n\to\mathbb{C}^n$ 为一个线性变换，设 $A=[a_{ij}]$为 T 关于标准基 $e_1,\ \cdots,\ e_n$ 的矩阵.

H (i)若$(,)$是$\mathbb{C}^n$ 上的埃尔米特型，试证存在线性变换 $T^\#:\mathbb{C}^n\to\mathbb{C}^n$ 满足

$$(Tu,v)=(u,T^\# v),$$

对所有 $u,\ v\in\mathbb{C}^n$.

H (ii)试证 $T^\#$ 关于标准基的矩阵是 $A^\#=[\overline{a}_{ji}]$(因此 $A^\#$ 是对 A^{T} 的每一个元素取共轭而得的矩阵．一个 $n\times n$的复矩阵 A 称为是埃尔米特的若 $A=A^\#$．当然每一个实对称矩阵是埃尔米特的).

H (iii)一个 $n\times n$ 的实矩阵 A 通过矩阵乘法：$T(v)=Av$ 定义了一个线性变换 $T:\mathbb{C}^n\to\mathbb{C}^n$. 试证若 A 是对称的，则 $T^\#=T$.

H (iv)试证$\mathbb{C}$ 上每一个埃尔米特矩阵 A 是可对角化的.

*4.55 若 A 是域 k 上的一个 $m\times n$ 的矩阵，试证 $\mathrm{rank}(A)\geq d$ 当且仅当 A 有一个非奇异的 $d\times d$ 的子矩阵．由此得出 $\mathrm{rank}(A)$是具有这样的性质的 d 的最大值.

*4.56 (i)若 A 和 B 是元素在一个交换环 R 中的 $n\times n$ 的矩阵，试证 $\mathrm{tr}(AB)=\mathrm{tr}(BA)$.

(ii)试用此习题的(i)给出推论 4.96 的另一个证明：若 A 和 B 是元素在域 k 中的相似矩阵，则 $\mathrm{tr}(A)=\mathrm{tr}(B)$.

4.57 若 A 是域 k 上的一个 $n\times n$ 的矩阵，其中 $n\geq 2$，试证 $\det(\mathrm{adj}(A))=\det(A)^{n-1}$.

*4.58 若 $g(x)=x+c_0$，则它的伴随矩阵 $C(g)$是 1×1 矩阵$[-c_0]$；若 $s\geq 2$ 且 $g(x)=x^s+c_{s-1}x^{s-1}+\cdots+c_1x+c_0$，则它的伴随矩阵 $C(g)$是 $s\times s$ 矩阵

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & 1 & \cdots & 0 & -c_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -c_{s-1} \end{bmatrix}$$

若 $C=C(g)$是 $g(x)\in k[x]$的伴随矩阵，试证 C 的特征多项式 $h_C(x)=\det(xI-C)=g(x)$.

*4.59 设 R 是一个交换环，若 A 是 R 上的一个 $n\times n$ 的矩阵，B 是 R 上的一个 $m\times m$ 的矩阵．则它们的直和定义为下面的$(m+n)\times(m+n)$的矩阵

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

若 A_1，…，A_t 是 R 上的方程，试证

$$\det(A_1 \oplus \cdots \oplus A_t) = \det(A_1) \cdots \det(A_t).$$

*H 4.60 若 A_1，…，A_t 和 B_1，…，B_t 是方阵，且对所有 i，A_i 相似于 B_i．试证 $A_1 \oplus \cdots \oplus A_t$ 相似于 $B_1 \oplus \cdots \oplus B_t$（矩阵的直和如习题 4.59 中的定义）. [398]

4.61 试证元素在域 k 中的一个 $n \times n$ 的矩阵 A 是奇异的当且仅当 0 是 A 的一个特征值.

H 4.62 设 A 为域 k 上的一个 $n \times n$ 的矩阵．若 c 是 A 的一个特征值，试证对所有 $m \geqslant 1$，c^m 是 A^m 的一个特征值.

4.63 求满足下条件的$\mathbb{R}$上的 $n \times n$ 的矩阵 A 的所有可能的特征值：A 和 A^2 是相似的.

4.64 $n \times n$ 的矩阵 N 称为**幂零的**若 $N^m = 0$，对某 $m \geqslant 1$．试证幂零矩阵的所有特征值是 0．应用凯莱-哈密顿定理去证其逆命题：若矩阵 A 的所有特征值均为 0，则 A 是幂零的.

H 4.65 若 N 是一个幂零矩阵，试证 $I + N$ 是非奇异的.

4.5 码

在习题 1.79 中讨论编码时，我们的重点是在安全上：我们如何才能防止一个未经授权的人获取我们的信息？为考虑获取的信息的准确度，现在我们离开侦探的世界，假设帕特问迈克要埃拉电话号码，但当迈克回答时一只狗在吠叫，由于这个噪声，帕特不确信他正确地听到了号码，因此他要求迈克重复一遍，有可能大多数情况下，一次或两次的重复才能保证帕特得到埃拉的电话号码．但是简单地重复一个信息数次可能是不可行的，地球上的科学家需要查看发自火星或木星的照片即是一个很好的例子．在 2004 年，送至这些星球的机器人照相机将每一个图片用下列的方式编码成一个二进制数字，一个图片被分成 1024×1024 的格点 p_{ij}（这是真实使用的数字），则有 $2^{10} \times 2^{10} = 2^{20} = 1\,048\,576$ 个格点．每一个格点带有一个 12-位的二进制数 c_{ij}，用于描述它的颜色、密度等等．$2^{10} \times 2^{10}$ 矩阵$[c_{ij}]$被写成一个 2-进制数：第一行，第二行，…，直至第 1024 行．在这种情况下，一张照片被转换为一个带有大约有 12 000 000 节的信息．此二进制数必须在太空中传播，而太空是“嘈杂的”，因为宇宙射线会干扰电磁信号．显然，传送如此长的信息穿越太空是不经济的，甚至即使被重复多次发送，也很有可能在直接收到的信息中没有两个会是一样的．像我们在埃拉的电话号码的例子中看到的，很自然地我们会重复地说，并且冗长码是准确接收的关键．我们来寻找一些可行的信息编码的方式，使得在接收信息时，错误能够被觉察，甚至更好，能够被修正，这就是使得我们有能力合理地看到从其他星球中传回的真实的图片而应做的.

4.5.1 分组码

码的数学研究是在二十世纪四十年代从香农(C. E. Shannon)、汉明(R. W. Hamming)和高雷(M. J. E. Golay)的工作开始的．将一个信息在一个嘈杂的渠道中传输涉及三步：对信息编码（编制冗余码）；传送信息，对接收的信息译码. [399]

记号 在此节中我们将用$\mathbb{B}$表示有限域$\mathbb{F}_2$.

→ **定义** 称一个有限集$\mathcal{A}$为一个**字母表**，它的元素为**字母**．若 m 和 n 是正整数，则一个编码

函数是一个单射函数 $E: \mathcal{A}^m \to \mathcal{A}^n$. $\mathcal{A}^m$ 或 $\mathcal{A}^n$ 中的元素 w 称为**字**，集合 $C = \mathrm{im}E \subseteq \mathcal{A}^n$ 称为 $\mathcal{A}$ 上的 $[n, m]$ **分组码**㊀，C 中的元素称为**码字**. 若 $\mathcal{A} = \mathbb{B}$，则一个 $[n, m]$ 分组码称为一个**二进制码**.

因为编码涉及冗余，这是通常在 $m<n$ 情形时出现的. m 的选择是不受限制的，因为任意一个长的信息可以细分成一些长度 $\leqslant m$ 的更短的子字. 一个传输的信息可能是从外层空间传至地球的一张照片，当然，这是我们想要看的. 如果在传输中没有干扰，则任何码字 $c=E(w)$ 可以如同 $w=E^{-1}(c)$ 一样被译码，因为编码函数是一个单射. 然而，因为有可能会出现错误，所以我们的任务是给一个码加上足够多的冗余码，使得人们能有效地从它的用于传输的版本中恢复出原来的码字.

→ **例 4.105** (i)**奇偶性校验 $[m+1, m]$ 码**

定义一个编码函数 $E: \mathbb{B}^m \to \mathbb{B}^{m+1}$ 为

$$w = (a_1, \cdots, a_m) \in \mathbb{B}^m \mapsto E(w) = (a_1, \cdots, a_m, b),$$

其中 $b = \sum_{i=1}^{m} a_i$. 显然 E 是一个单射，易证码 $C = \mathrm{im}E \subseteq \mathbb{B}^{m+1}$ 如下给出：

$$C = \{(b_1, \cdots, b_{m+1}) \in \mathbb{B}^{m+1} : b_1 + \cdots + b_{m+1} = 0\}.$$

设 $w \in \mathbb{B}^m$，则 $E(w)$ 的**奇偶性**为偶若它的坐标的和在 $\mathbb{B}$ 中为 0. 如果人们收到一个奇偶性为奇的信息(即坐标的和为 1)，这样人们知道在传输中一定出现了一个错误，因此此码可以觉察出单个错误的存在. 然而，在收到的信息中若有一对错误，则不能被觉察出，因为此时奇偶性未变. 例如，两个 0 被换成两个 1.

(ii)**三重重复 $[12, 4]$ 码**

考虑定义为 $E(w) = (w, w, w)$ 的编码函数 $E: \mathbb{B}^4 \to \mathbb{B}^{12}$，也就是，$C$ 由如下形式的字组成：

400

$$E(a_1, a_2, a_3, a_4) = (a_1, a_2, a_3, a_4, a_1, a_2, a_3, a_4, a_1, a_2, a_3, a_4).$$

现在传输 (a_1, a_2, a_3, a_4)，设收到的信息为 $y = (r_1, \cdots, r_{12})$. 由于干扰，有可能

$$(r_1, \cdots, r_{12}) \neq E(a_1, a_2, a_3, a_4).$$

对收到的字 $y = (r_1, \cdots, r_{12})$ 译码如下：若在传输中无错误，则 $r_1 = r_5 = r_9$. 因为 r_1, r_5, r_9 的取值只有两种可能，因此在任何情形下，它们的值至少有两个是相等的. 定义 b_1 为这个取的最多的值. 类似地，定义 b_2, b_3 和 b_4，因此 y 被译码为 (b_1, b_2, b_3, b_4)(因为信息必须被译码，我们不考虑二重重复 $[8, 4]$ 码，这是因为比如，若 $r_1 \neq r_5$，译码 $(r_1, \cdots, r_8)$ 时，就不存在自然的候选). 注意这种编码方案可以检查出错误：若 r_i, r_{i+4}, r_{i+8} 不全等，则存在一个错误(哎！真的遭糕的错误也许没被觉察出来). 事实上，此码在该意义下可纠正一个错误：若收到的信息 y 含有一个错误，则 y 可以替换成除一个字母外其余与 y 的字母一样的码字.

(iii)**二维奇偶性 $[9, 4]$ 码.**

记字 $y = (r_1, \cdots, r_9) \in \mathbb{B}^9$ 为一个 3×3 的矩阵

$$\begin{bmatrix} r_1 & r_2 & r_3 \\ r_4 & r_5 & r_6 \\ r_7 & r_8 & r_9 \end{bmatrix}.$$

㊀ 称之为分组码是因为所有码字具有相同的长度，即 n. 我们可以很容易地修改分组码以允许不同长度的字.

考虑如下定义的编码函数 $E: \mathbb{B}^4 \to \mathbb{B}^9$：

$$E(a,b,c,d) = \begin{bmatrix} a & b & r_3 \\ c & d & r_6 \\ r_7 & r_8 & r_9 \end{bmatrix} = \begin{bmatrix} a & b & a+b \\ c & d & c+d \\ a+c & b+d & a+b+c+d \end{bmatrix}.$$

因此 r_3 和 r_6 是头两行的奇偶校验，r_7 和 r_8 是头两列的奇偶校验，而 r_9 既是 r_7 和 r_8 也是 r_3 和 r_6 的奇偶校验．我们就构造了一个由 $\mathbb{B}$ 上的所有行和列均为偶的 3×3 矩阵组成的[9，4]-码 $C=\mathrm{im}E$．假设收到的矩阵是

$$y = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

我们觉察到第二行有一个错误，第一列也一样，因为它们的和在 $\mathbb{B}$ 中不等于 0．因此在(2，1)位的元素的错误被发现，从而可以改正之．现在我们证明 2 个错误也能被发现．例如，假设收到的矩阵是

$$y' = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$ 401

在行上的奇偶校验是正确的，但奇偶校验检查出了在开始两列中的错误．

将三重重复[12，4]码与此码作比较．我们发现将一个长度为 4 的字编码成一个长度为 9 的字比编码成一个长度为 12 的字的效率更高．◀

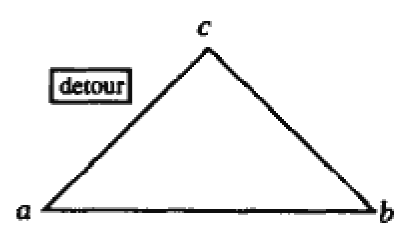


图 4-8　三角不等式

我们来度量 $\mathcal{A}^n$ 中字之间的距离．

定义　设 X 是一个集合，X 上的一个**度量**是满足下列条件的一个函数 $\delta: X\times X \to \mathbb{R}$

(i) $\delta(a,b)\geqslant 0$，对所有的 a，$b\in X$ 且 $\delta(a,b)=0$ 当且仅当 $a=b$；

(ii) $\delta(a,b)=\delta(b,a)$，对所有的 a，$b\in X$；

(iii) **三角不等式**：

$$\delta(a,b) \leqslant \delta(a,c)+\delta(c,b), \text{对所有的 } a,b,c \in X.$$

度量具有距离这个特定概念的本质的性质．距离是非负的(两个点不能相距-5 个单位)．两个不同点的距离应该是正的．乌尔巴纳到芝加哥的距离与芝加哥到乌尔巴纳的距离应该是一样的．三角不等式是说两点之间"直线"是最短的路．

例 4.106　(i)若 $X=\mathbb{R}$，则 $\delta(x,y)=|x-y|$ 是一个度量．

这就是在微积分中引入绝对值的原因．在此情形下，点 z 在 x 和 y 之间当且仅当 $\delta(x,y)=\delta(x,z)+\delta(z,y)$．

(ii)**欧几里得度量**．

若 $X=\mathbb{R}^n$，$x=(x_1,\cdots,x_n)$，$y=(y_1,\cdots,y_n)$，则 $\delta(x,y)=\sqrt{\sum_{i=1}^{n}(x_i-y_i)^2}$ 是一个度量．注

402 意 $\sqrt{x^2}=|x|$,因此当 $n=1$ 时,此定义与(i) 中的定义一致.

(iii)L^2 **度量.**

设 $L^2[a,b]$表示所有平方可积函数构成的集合,也就是 $L^2[a,b]=\{f:[a,b]\to\mathbb{R}:\int_a^b f^2(x)\mathrm{d}x<\infty\}$. 则

$$\delta(f,g)=\sqrt{\int_a^b (f(x)-g(x))^2\mathrm{d}x}$$

是 $L^2[a,b]$上的一个度量.

(iv)p-**进制度量**

若 p 是一个素数,$n\in\mathbb{Z}$ 是非零的,则 $n=p^k u$,其中 $k\geqslant 0$ 且 $p\nmid u$,即 p^k 是整除 n 的 p 的最大的方幂. 记 $k=k(n)$. 若我们定义若 $n\neq m$,$\delta(n,n)=0$ 且 $\delta(n,m)=p^{-k(n-m)}$,则 δ 是$\mathbb{Z}$上的一个度量. ◀

定义 设$\mathcal{A}$是一个字母表,$w=(a_1,\cdots,a_n)$,$w'=(a_1',\cdots,a_n')\in\mathcal{A}^n$. 定义函数 $\delta:\mathcal{A}^n\times\mathcal{A}^n\to\mathbb{R}$ 如下:

$$\delta(w,w')=\text{满足 } a_i\neq a_i' \text{的 } i \text{ 的个数},$$

称之为**汉明距离**[⊖].

→ **命题 4.107** 若$\mathcal{A}$是一个字母表,$n\geqslant 1$,则汉明距离是$\mathcal{A}^n$上的一个度量.

证明 设 $w=(a_1,\cdots,a_n)$,$w'=(a_1',\cdots,a_n')\in\mathcal{A}^n$. 显然,$\delta(w,w')\geqslant 0$ 且 $\delta(w,w)=0$. 另一方面,若 $\delta(w,w')=0$,则对所有的 i 有 $a_i=a_i'$,从而 $w=w'$. 显然 $\delta(w,w')=\delta(w',w)$,因此只剩下三角不等式要证.

若我们定义 $\delta_i(w,w')=1$ 若 $a_i\neq a_i'$;$\delta_i(w,w')=0$ 若 $a_i=a_i'$,则

$$\delta(w,w')=\sum_{i=1}^{n}\delta_i(w,w').$$

只需证明对每一个 i 有 $\delta_i(w,w')\leqslant\delta_i(w,z)+\delta_i(z,w')$,其中 $z=(b_1,\cdots,b_n)$. 若 $\delta_i(w,w')=0$,则此不等式成立. 否则 $\delta_i(w,w')=1$. 而 $\delta_i(w,z)+\delta_i(z,w')$为 0,1 或 2 中之一,故只须证明 $\delta_i(w,z)+\delta_i(z,w')\neq 0$. 若此和为 0,则 $\delta_i(w,z)=0=\delta_i(z,w')$,也就是 $a_i=b_i$,
403 $b_i=a_i'$. 然而若 $\delta_i(w,w')=1$,则 $a_i\neq a_i'$,矛盾. ■

→ **定义** 若$\mathcal{A}$是一个字母表,$C\subseteq\mathcal{A}^n$是一个码,则它的**最小距离**是

$$d=d(C)=\min_{w,w'\in C,w\neq w'}\delta(w,w'),$$

其中 $\delta(w,w')$是汉明距离.

最小距离是非常重要的概念,它通常编入用于描述码的参数中.

记号 **$\mathcal{A}$上的一个(n,M,d)-码**指的是码 $C\subseteq\mathcal{A}^n$,其中$\mathcal{A}$是一个字母表,$M=|C|$,d 是它的最小距离.

注意,若 $|\mathcal{A}|=q$,则 $M=q^m$,因为编码函数 $E:\mathcal{A}^m\to\mathcal{A}^n$是一个单射. 因此如果用我们以前的记号的话,一个$(n,M,d)$-码就是一个$[n,\log_q M]$-码.

⊖ 为纪念汉明(R. W. Hamming)而命名.

现在我们给出查错与纠错的准确定义.

→ **定义** 设$\mathcal{A}$是一个字母表，$C\subseteq\mathcal{A}^n$是一个码. 码 C 可以**查 $s>0$ 个错**若在至多 s 处改变一个码字 $c\in C$ 不会得到一个码字.

例如，奇偶性检验$[m+1, m]$-码可以查 1 个错，因为改变一个码字的一个坐标就可将一个偶字转变成一个奇字.

一个码 C 可查 s 个错，若对每一个 $c\in C$ 和 $y\in\mathcal{A}^n$，从 $0<\delta(y, c)\leqslant s$ 可推出 $y\notin C$.

→ **定义** 设$\mathcal{A}$是一个字母表，$C\subseteq\mathcal{A}^n$是一个码. 若 $y\in\mathcal{A}^n$，则称 $c\in C$ 是一个与 y **最靠近的码字**，若对所有的 $c'\in C$ 有 $\delta(y, c)\leqslant\delta(y, c')$.

对给定的 y，可以不存在唯一的与 y 最靠近的码字(习题 4.73 要求给出一个例子，使得不同的码字与一个字等距). 当一个接收到的字 y 的确有唯一的最靠近的码字 c 时，则我们就将 y 译为 $E^{-1}(c)$. 我们不是说 $c=E(w)$，但它是真实解的最好(并且是最自然)的候选.

→ **定义** 设$\mathcal{A}$是一个字母表，$C\subseteq\mathcal{A}^n$是一个码. 称码 C **可纠 t 个错**，若在至多 t 处改变一个码字 c，得出一个字 $y\in\mathcal{A}^n$且 y 的唯一最靠近的码字为 c.

因此，一个码 C 可纠 t 个错，若给定的一个码字 c 和满足 $\delta(y, c)\leqslant t$ 的一个字 y，则对每一个码字 $c'\neq c$，均有 $\delta(y, c)<\delta(y, c')$. 404

→ **命题 4.108** 设$\mathcal{A}$是一个字母表，$C\subseteq\mathcal{A}^n$是一个(n, M, d)-码.

(i)设 $d\geqslant 2t+1$ 且 $y\in\mathcal{A}^n$. 如果满足 $\delta(y, c)\leqslant t$ 的码字 $c\in C$ 存在的话，则它一定唯一.

(ii)若 $d\geqslant s+1$，则 C 可以查 s 个错.

(iii)若 $d\geqslant 2t+1$，则 C 可纠 t 个错.

证明 (i)假设 c，c'是满足$\delta(y, c)=\delta(y, c')\leqslant t$ 的码字. 则由三角不等式有 $\delta(c, c')\leqslant\delta(c, y)+\delta(y, c')\leqslant 2t$. 但不同码字之间的最小距离是 $d(C)\geqslant 2t+1$. 因此 $c=c'$.

(ii)若 $w\neq c$ 与 c 至多在 s 处不同，则 $0<\delta(c, w)\leqslant s$. 但若 $w\in C$，则

$$s\geqslant\delta(c,w)\geqslant d>s$$

矛盾.

(iii)若 w 是改变 c 的至多 t 处而得，则 $\delta(c, w)\leqslant t$. 若存在一个码字 c'满足 $\delta(c', w)<\delta(c, w)$，则由三角不等式得

$$\begin{aligned}2t+1&\leqslant d\\&\leqslant\delta(c,c')\\&\leqslant\delta(c,w)+\delta(w,c')\\&\leqslant 2\delta(c,w)\leqslant 2t.\end{aligned}$$

此矛盾表明 C 可纠 t 个错. ∎

→ **例 4.109** (i)例 4.105(i)的奇偶性检验$[m+1, m]$-码是一个$(m+1, 2^m, 2)$-码，它是由B^{m+1}中的所有具有偶数个 1 的字构成的. 极小距离至少是 2，因为改变具有偶数个 1 的字一处，则产生一个具有奇数个 1 的字. 由命题 4.108(ii)，此码可查 1 个错，然而不能纠错.

(ii)例 4.105(ii)的三重重复$[3m, m]$-码由B^{3m}中形如(w, w, w)的字组成，其中 $w\in\mathrm{B}^m$. 它是一个$(3m, 2^m, 3)$-码，因为我们必须至少改变一个码字的 3 处才能获得另一个码字. 由例

题 4.108(iii)知，此码能够查 2 个错，此码也能纠 1 个错.

(iii)在例 4.105(iii)中，二维奇偶性[9, 4]-码 C 是由$\mathbb{B}$上所有每一行的元素的和与每一列的元素的和均为 0 的 3×3 的矩阵组成. 习题 4.67 要求读者验证，将一个码字(此处是一个矩阵)变
405 成另一个码字至少需要改变 3 处. 因此 $d\geqslant 4$. 因此 C 能查 2 个错，C 也可以纠 1 个错. ◀

一个码若具有大的极小距离 d，则它可纠多个错. 例如，一个 101－次二重重复码 C 是 $[101m, m]$-码，其编码函数 $E: \mathbb{B}^m\to\mathbb{B}^{101m}$将一个 m 位字重复 101 次. 此时 $d=101$，因此由命题 4.108(iii)知，C 可纠 50 个错. 显然 C 是一个非常不切合实际的码. 我们可测量这种实际性.

定义 一个$[n, m]$-码的**信息率**规定为$\frac{m}{n}$. 若 $|\mathcal{A}|=q$，则我们知道 $M=q^m$，因此一个 (n, M, d)-码的**信息率**是$(\log_q M)/n$.

信息率是一个很自然的概念：它表示的是 n 个字母被用于发送 m 位的信息. 刚刚描述的多重重复$[101m, m]$-码的效率是低的，因为它的信息率是$\frac{1}{101}$：发送一个短的信息需要数量庞大的字母. 另一方面，无冗余$[m, m]$-码 $E=1_{\mathcal{A}^m}: \mathcal{A}^m\to\mathcal{A}^m$的信息率为 1，它仅仅是毫无改动地重复信息. 因此，信息率小的码能纠多个错，但它们是效率低的；而信息率大的(接近 1)码不能查错. $\mathcal{A}$上的(n, M, d)-码可纠 t 个错若 $d\geqslant 2t+1$. 因此，当 d 越大，它越精确. 习题 4.68 定义了单字界：若 $|\mathcal{A}|=q$，则 $M=q^m\leqslant q^{n-d+1}$. 因此 $m+d\leqslant n+1$ 且$\frac{m}{n}+\frac{d}{n}\leqslant 1+\frac{1}{n}$. 若 m 很大，则比率$\frac{m}{n}$接近 1，但此时 d 较小. 另一方面，若 m 较小，则信息率也小，但此时 d 可能较大，也就是，此码可以纠正多个错. 因此，我们寻找一个折衷的比率. 给定 d，我们寻找 (n, q^m, d)-码，使得其中 m"较大"——这样的码相对地更有效些；给定 m，我们寻找(n, q^m, d)-码，使得其中 d"较大"——这样的码相对地更准确些.

4.5.2 线性码

设$\mathcal{A}$是任一集合，函数 $E: \mathcal{A}^m\to\mathcal{A}^n$的定义可能很复杂. 另一方面，若$\mathcal{A}$是一个域，则$\mathcal{A}^m$和$\mathcal{A}^n$是带有标准基的向量空间. 进一步，若 E 是一个线性变换，则用下面的公式可高效地描述它：存在一个 $m\times n$ 矩阵 G 使得 $E(w)=wG$，其中 w 是一个 $1\times m$ 的行向量.

→ **定义** 有限域 k 上的一个$[n, m]$-**线性码** C 指的是 k^n 的一个 m 维子空间. C 的一个**编码函数** $E: k^m\to k^n$ 是一个满足 $E(k^m)=C$ 的单射线性变换.

若 $k=\mathbb{F}_q$ 是一个具有 q 个元素的有限域，则一个$[n, m]$-线性码就是一个(n, q^m, d)-码，
406 其中 d 是极小距离. 在一个线性码中，有另一种方法求它的极小距离.

→ **定义** 若 $w=(a_1, \cdots, a_n)\in k^n$，其中 k 是一个域，则 w 的**支撑**定义为

$$\mathrm{Supp}(w) = \{指标\ i: a_i\neq 0\}.$$

若 C 是一个线性(n, M, d)-码，则 w **的汉明权**是

$$\mathrm{wt}(w) = |\mathrm{Supp}(w)|;$$

也就是，$\mathrm{wt}(w)$是 w 中非零坐标的个数. w 的**零集**是 $\mathrm{Supp}(w)$的补集：

$$\mathcal{Z}(w)=\{\text{指标 } i: a_i=0\}.$$

注意 $\mathrm{wt}(w)=\delta(w, 0)$，其中 δ 是汉明距离，且 $0=(0, \cdots, 0)$（它在 C 中，因为 C 是 k^n 的一个子空间）.

→ **命题 4.110** *若 C 是有限域 $\mathbb{F}_q$ 上的一个线性 (n, M, d)-码，则*

$$d=\min_{c\in C, c\neq 0}\{\mathrm{wt}(c): c\in C\}.$$

因此，d 是非零码字的最小权数.

证明 因为 C 是一个子空间，所以由 $w, w'\in C$ 可推出 $w-w'\in C$，因此

$$\begin{aligned}d&=\min_{w,w'\in C, w\neq w'}\delta(w,w')\\&=\min_{w,w'\in C, w\neq w'}\{\mathrm{wt}(w-w'): w,w'\in C\}\\&=\min_{c\in C, c\neq 0}\{\mathrm{wt}(c): c\in C\}\end{aligned}$$ ■

我们来引入一个可描述给定线性码的矩阵，为此先介绍关于一个矩阵 U 的划分.

记号 设 A 是一个 $m\times r$ 的矩阵，B 是一个 $m\times s$ 的矩阵，则

$$U=[A\mid B]$$

是一个 $m\times(r+s)$ 的矩阵，它的头 r 列为矩阵 A，后 s 列是矩阵 B.

若 N 是一个 $q\times m$ 的矩阵，A 是一个 $m\times r$ 的矩阵，则由矩阵乘法，NA 的 (i, j)-元素是点积：$\mathrm{ROW}_N(i)\cdot\mathrm{COL}_A(j)$. 因此 NA 的第 j 列与 A 的 $\mathrm{COL}_A(j)$ 之外的列无关. 因此得出，若 $U=[A\mid B]$，则

$$N[A\mid B]=[NA\mid NB]. \tag{1}$$ 407

因为在码理论中我们习惯于将 k^m 中的向量看成行向量，而不是列向量（与前面的章节不同）. 因此以后我们将元素 $w\in k^n$ 视为 $1\times n$ 的行向量，而 $n\times 1$ 列向量记为 w^{T}.

设 $\sigma\in S_n$ 是一个置换，Q_σ 是对单位矩阵用 σ 置换其列而得的 $n\times n$ 的置换矩阵. 若 k 是一个域，$c=(c_1, \cdots, c_n)\in k^n$ 是一个 $1\times n$ 的行向量，则

$$cQ_\sigma=(c_1,\cdots,c_n)Q_\sigma=(c_{\sigma(1)},\cdots,c_{\sigma(n)});$$

第 cQ_σ 的第 j 个坐标是 c 与 Q_σ 的第 j 列的点积. 但若 $e_{\sigma(j)}$ 是在 $\sigma(j)$ 位的坐标为 1 其余为 0 向量，则 $c\cdot e_{\sigma(j)}=(c_1, \cdots, c_n)\cdot(0, \cdots, 1, \cdots, 0)$. 因此 $c\cdot e_{\sigma(j)}=c_{\sigma(j)}$. 若 Q_σ 是一个 $n\times n$ 的置换矩阵，则定义 $\sigma_*: k^n\to k^n$ 为

$$\sigma_*(c)=cQ_\sigma.$$

定义 域 k 上两个 $[n, m]$-线性码 C，C' 是**置换等价的**，若存在 $\sigma\in S_n$ 使得 $\sigma_*(C)=C'$. 也就是，$c=(a_1, \cdots, a_n)\in C$ 当且仅当 $(a_{\sigma(1)}, \cdots, a_{\sigma(n)})\in C'$.

易见置换等价是 k^n 中所有线性码的一个等价关系，置换等价的码实质上是一样的：例如，若一个码 C 中的所有字被翻转过来，则新的线性代码与原来的码具有相同的参数.

→ **命题 4.111** *若 C 是域 k 上的一个线性 $[n, m]$-码，则存在置换等价于 C 的线性码 C' 和一个具有形式 $G=[I\mid B]$ 的 $m\times n$ 的矩阵 G，其中 I 是 $m\times m$ 的单位矩阵，使得*

$$C'=\{w'G: w'\in k^m\}.$$

因此，C' 是矩阵 G 的行空间.

证明 若 e_1，…，e_m 是 k^m 的标准基，γ_1，…，γ_m 是 C 的某组基. 由 $E(e_i)=\gamma_i$ 定义一个线性变换 $E: k^m \to k^n$. 由引理 4.77(iii)知 E 是一个单射. 事实上，E 是一个同构 $k^m \to C$. 由命题 4.64，$E(w)=Aw^T$，其中 $w\in k^m$ 是一个 $1\times m$ 的行向量，而 A 是列为向量 $E(e_i)^T$ 的 $n\times m$ 的矩阵. 因为我们将 k^m 中的元素看成行向量而不是列向量，故我们可记 $E(w)=wN$，其中 $N=A^T$ 是一个 $m\times n$ 的矩阵.

由命题 4.39，高斯消元法将矩阵 N 转变为一个阶梯形矩阵 G. 存在一个非奇异的 $m\times m$ 的矩阵 P 和一个 $n\times n$ 的置换矩阵 Q_σ 使得 $G=PNQ_\sigma=[U \mid B]$，其中 U 是一个阶梯形矩阵，B 是一个 $m\times(n-m)$ 的矩阵. 因为 E 是一个单射，所以阶梯形矩阵 U 无零行，因此它是一个单位矩阵，从而 $G=[I \mid B]$. 定义

408 $$C' = \{w'G : w' \in k^m\}.$$

注意 e_1G，…，e_mG 是一个线性无关的表，所以 $m\leqslant \dim(C')$. 我们断言 C 和 C' 是置换等价的，也就是 $C'=\sigma_*(C)$. 设 $c'=w'G\in C'$，定义 $w=w'P$ 并且定义 $c=wN$. 注意 $c\in C$ 因为 $wN=E(w)\in C$. 则有：

$$\begin{aligned} c' &= w'G \\ &= w'PNQ_\sigma \\ &= wNQ_\sigma \\ &= cQ_\sigma \\ &= \sigma_*(c). \end{aligned}$$

因此，$C'\subseteq\sigma_*(C)$. 从而 $m\leqslant\dim(C')\leqslant\dim(\sigma_*(C))=\dim(C)=m$. 由推论 4.25(iii)，我们有 $C'=\sigma_*(C)$. 所以 C 和 C' 是置换等价的码. ■

→ **定义** 若 C 是域 k 上的一个$[n, m]$线性码，则满足 $C=\mathrm{ROW}(G)=\{wG : w\in k^n\}$ 的 $m\times n$ 的矩阵 G 称为 C 的**生成矩阵**. C 的**阶梯形生成矩阵**是具有形式 $G=[I \mid B]$ 的生成矩阵，其中 I 是 $m\times m$ 的单位矩阵.

每一个线性码 C 有一个生成矩阵：例如，任一个由其行向量构成 C 的一组基的 $m\times n$ 的矩阵就是 C 的一个生成矩阵. 应用命题 4.111，我们可以假设每一个线性码都有一个阶梯形生成矩阵.

事实上，到目前为止我们给出的码的例子只有二元线性码，也就是说，这些码是 $k=\mathrm{B}=\mathbb{F}_2$ 上的线性码.

→ **例 4.112** (i)考虑例 4.105(i)中的奇偶性检验$[m+1, m]$码 C. 码字是所有满足 $\sum b_i=0$ 的 $c=(b_1, \cdots, b_{m+1})\in\mathrm{B}^{m+1}$. 这些码所构成一个子空间. 因此 C 是一个线性码：回忆到它的编码函数 E：$\mathrm{B}^m\to\mathrm{B}^{m+1}$ 定义如下

$$E:(a_1,\cdots,a_m)\mapsto(a_1,\cdots,a_m,b),$$

其中 $b=\sum_{i=1}^{m}a_i$. 易见 E 是一个线性变换. 进一步，一个阶梯形生成矩阵是如下的 $m\times(m+1)$ 的矩阵

$$G=\begin{bmatrix}1&0&0&\cdots&0&1\\0&1&0&\cdots&0&1\\&\vdots&\vdots&\vdots&\vdots&\\0&0&0&\cdots&1&1\end{bmatrix}.$$

用划分记号，$G=[I \mid B]$，其中 I 是 $m\times m$ 的单位矩阵，B 是所有元素为 1 的列向量. 409

(ii)考虑例 4.105(ii)中的二维奇偶性[9，4]-码.

由定义，

$$E:(a,b,c,d)\mapsto\begin{bmatrix}a&b&a+b\\c&d&c+d\\a+c&b+d&a+b+c+d\end{bmatrix}.$$

易证 E 是一个线性变换. 求 E 在$\mathbb{B}^4$ 的标准基上的值可得出一个生成矩阵 G，因为 G 的第 i 行是 e_iG.

$$G=\begin{bmatrix}1&0&0&0&1&0&1&0&1\\0&1&0&0&1&0&0&1&1\\0&0&1&0&0&1&1&0&1\\0&0&0&1&0&1&0&1&1\end{bmatrix}.$$

因此 G 是一个阶梯形生成矩阵.

(iii)考虑例 4.105(ii)中的三重重复$[3m, m]$-码. C 的阶梯形生成矩阵是$G=[I \mid I \mid I]$，其中 I 是 $m\times m$ 的单位矩阵.

(iv)上面的例子太简单了. 给定一个线性$[n, m]$-码 C，其编码函数为 $E: k^m\to k^n$，行为 $E(e_1)$，…，$E(e_m)$的矩阵 G 是 C 的生成矩阵(其中 e_1，…，e_m 为 k^m 的标准基). 一般地，将 G 化成 C 的(或置换等价于 C 的线性码 C'的)一个阶梯形生成矩阵时需要用高斯消元法. ◀

若 $G=[I \mid B]$是线性$[n, m]$-码 C 的一个阶梯形生成矩阵，则对所有的 $w\in k^m$，前面的等式(1)给出

$$wG=w[I \mid B]=[w \mid wB].$$

若在传输 C 时没有错误，则如何译一个码字 wG 是显然的：仅仅是取它的头 m 个坐标. 一个阶梯形生成矩阵 $G=[I \mid B]$的后 $n-m$ 列应该被视为例 4.112(i)中奇偶性$[m+1, m]$检验码的阶梯形生成矩阵的最后一列的推广. 因此 $G=[I \mid B]$的后几列 B 是推广的奇偶性检验，它提供冗余码以有助于译出一个嘈杂通道传递的码.

在例 4.12 中，我们从一些线性码开始并对每一个码都求出了一个阶梯形生成矩阵，现在我们从一个阶梯形生成矩阵 G 开始，用它去构造一个码 $C=\{wG: w\in k^m\}$.

→ **例 4.113** 考虑 4×7 的矩阵

$$G=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix},$$ 410

定义**汉明[7, 4]-码**为 $C=\{wG: w\in \mathbb{B}^4\}$.

显然，信息率是 $r=\frac{4}{7}$. 我们来计算 C 的最小距离 d. 记 G 的行为 γ_1, γ_2, γ_3, γ_4. 因为此时 $k=\mathbb{B}$，所以线性组合 $\sum_i a_i\gamma_i$ 就是行的和(因为 a_i 是 0 或 1). 由命题 4.110，我们可以通过计算码字的权来计算 d. 注意

$$\mathrm{wt}(\gamma_1)=3;\mathrm{wt}(\gamma_2)=3;\mathrm{wt}(\gamma_3)=3;\mathrm{wt}(\gamma_4)=4.$$

G 中两行的和共有 $\binom{4}{2}=6$ 个，此时一个简短的计算表明最小权数是 3. G 的 3 行的和有 $\binom{4}{3}=4$ 个，最小权数是 3；所有 4 行的和的权为 7. 我们得到结论 C 的最小距离是 3，因此 C 可以查 2 个错. 由命题 4.108(iii)可知码 C 也可以纠 1 个错. 计算 $d(C)$的另一种方法参见例 4.117.

此构造也可以推广. 若 $\ell\geqslant 3$，则在$\mathbb{B}^\ell$ 中存在 $2^\ell-1$ 个非零的字. 定义一个$(2^\ell-1-\ell)\times(2^\ell-1)$的矩阵 $G=[I\mid B]$，其中 B 的行是由所有满足 $\mathrm{wt}(w)\geqslant 2$ 的 $w\in\mathbb{B}^{2^\ell-1-\ell}$组成的. 定义**汉明$[2^\ell-1, 2^\ell-1-\ell]$-码**为 $C=\{wG: w\in\mathbb{B}^{2^\ell-1-\ell}\}$. 当然，$G$ 是 C 的一个阶梯形生成矩阵. 汉明码的信息率是

$$\frac{2^\ell-1-\ell}{2^\ell-1}=1-\frac{\ell}{2^\ell-1};$$

当 ℓ 变大时，第 ℓ 次汉明码的信息率非常接近 1. 与在[7, 4]-码中一样，可以证明每一个汉明码的极小距离是 3. ◀

下面的命题给出一个测试一个字是否为码字的准则.

→ **命题 4.114** 设 $G=[I\mid B]$是域 k 上一个线性$[m+p, m]$码的 $m\times(m+p)$的阶梯形生成矩阵(因此 B 是一个 $m\times p$ 的矩阵)，则 $w\in k^{m+p}$落在 C 中当且仅当 $w[-B^{\mathrm{T}}\mid J]^{\mathrm{T}}=0$，其中 J 是 $p\times p$ 的单位矩阵.

证明 记$(m+p)\times p$ 的矩阵$[-B^{\mathrm{T}}\mid J]$为 H. 因为 C 是 G 的行空间，所以每一个码字 c 是G 的行的一个线性组合. 但 G 的第 i 行是 e_iG，其中 e_1, …, e_m 是 k^m 的标准基(在此节中，k^m 中的元素均被视为 $1\times m$ 的行向量)，所以 $c=\sum_i a_i(e_iG)$,其中 $a_i\in k$. 因此只须证明 $GH^{\mathrm{T}}=0$,因为这样的话 $cH^{\mathrm{T}}=\sum_i a_ie_iGH^{\mathrm{T}}=0$.

v, $w\in k^{m+p}$的点积等于矩阵的乘积：$v\cdot w=vw^{\mathrm{T}}$. 特别地，GH^{T} 的 ij 位元素是 $\mathrm{ROW}_G(i)\cdot\mathrm{COL}_{H^{\mathrm{T}}}(j)=\mathrm{ROW}_G(i)\mathrm{COL}_{H^{\mathrm{T}}}(j)^{\mathrm{T}}$，$G$ 的第 i 行是

411

$$\mathrm{ROW}_G(i)=e_iG=e_i[I\mid B]=[e_i\mid e_iB]=(e_i,b_{i1},b_{i2},\cdots,b_{ip}).$$

H^{T} 的第 j 列是 $H^{\mathrm{T}}(e'_j)^{\mathrm{T}}$，其中 e'_1, …, e'_p是 k^p 的标准基，且$(e'_j)^{\mathrm{T}}$ 是一个列向量. 注意

$$H^{\mathrm{T}}(e'_j)^{\mathrm{T}}=[-B^{\mathrm{T}}\mid J]^{\mathrm{T}}(e'_j)^{\mathrm{T}}=(e'_j[-B^{\mathrm{T}}\mid J])^{\mathrm{T}}=[-e'_jB^{\mathrm{T}}\mid e'_j]^{\mathrm{T}}.$$

但 e'_jB^{T} 是 B^{T} 的第 j 行，它是 B 的第 j 列. 因此

$$\mathrm{COL}_{H^{\mathrm{T}}}(j)=(-b_{1j},-b_{2j},\cdots,-b_{pj},e'_j)^{\mathrm{T}}.$$

且

$$\mathrm{COL}_{H^{\mathrm{T}}}(j)^{\mathrm{T}}=(-b_{1j},-b_{2j},\cdots,-b_{pj},e'_j).$$

因此 GH^T 的 ij 位元素是

$$
\begin{aligned}
\mathrm{ROW}_G(i)\cdot\mathrm{COL}_{H^T}(j) &= \mathrm{ROW}_G(i)(\mathrm{COL}_{H^T}(j))^T \\
&= (e_i, b_{i1}, b_{i2}, \cdots, b_{ip})\cdot(-b_{1j}, -b_{2j}, \cdots, -b_{pj}, e'_j) \\
&= b_{ij} - b_{ij} \\
&= 0
\end{aligned}
$$

因此，$GH^T=0$，且 $cH^T=c[-B^T \mid J]^T=0$，得证.

反之，考虑齐次方程组 $[-B^T \mid J]^T x^T=0$ 和它的解空间 $S=\{v^T\in k^{m+p}: [-B^T \mid J]^T v^T=0\}$. 注意 $v\in S$ 当且仅当 $v[-B^T \mid J]=0$，因此由此证明的第一部分即有 $C\subseteq S$. 但 $\dim(C)=m$，而 $\dim(S)=m+p-r$，其中 $r=\mathrm{rank}([-B^T \mid J]^T)=p$. 由定理 4.43，我们有 $\dim(S)=m+p-p=m$，所以由推论 4.25，$C=S$. 因此，若 $w[-B^T \mid J]^T=0$，则 $w\in S$，从而 $w\in C$. ■

→ **定义** 设 C 是域 k 上的一个线性$[(m+p), m]$-码，一个 $m\times(m+p)$ 的矩阵 H 称为 C 的一个**奇偶性检验矩阵**，若对所有的 $w\in k^{m+p}$，我们有 $wH^T=0$ 当且仅当 $w\in C$.

命题 4.114 说，若 $G=[I \mid B]$ 是线性$[(m+p), m]$-码 C 的一个 $m\times(m+p)$ 的阶梯形生成矩阵，则 $H=[-B^T \mid J]$ 是 C 的一个奇偶性检验矩阵. 像我们在命题 4.132 中看到的一样，C 的奇偶性检验矩阵不必唯一.

注 若 $C\subseteq k^n$ 是一个码，定义它的**对偶码**为正交补

$$C^{\perp}=\{y\in k^n:(y,c)=0,\text{对所有的 } c\in C\},$$

其中 $(y, c)=y_1c_1+\cdots+y_nc_n$ 是 $y=(y_1, \cdots, y_n)$ 和 $c=(c_1, \cdots, c_n)$ 的普通点积. 应用命题 4.114，可证明若 $G=[I \mid B]$ 是 C 的一个生成矩阵，则奇偶性检验矩阵 $H=[-B^T \mid J]$ 是对偶码 $C^{\perp}$ 的一个生成矩阵.

下面的推论是用一个与奇偶性检验矩阵相关的奇妙的数来计算线性码 C 的最小权数 $d(C)$. 412

定义 若 A 是域上的一个 $m\times n$ 的矩阵，其中 $m<n$，则由它的列组成的表是线性相关的. 定义

$$\mu(A)=A\text{ 的线性相关的列的最小列数}.$$

若 A 是一个 $m\times n$ 的矩阵，$m<n$ 和 $\mathrm{rank}(A)=r$，则任意 $r+1$ 列是线性相关的. 因此

$$\mu(A)\leqslant r+1. \tag{2}$$

例 4.115 考虑矩阵

$$A=\begin{bmatrix}1&0&1&0\\0&1&0&0\end{bmatrix},\quad B=\begin{bmatrix}1&0&1&1\\0&1&0&0\end{bmatrix},\quad C=\begin{bmatrix}1&0&1&-1\\0&1&1&1\end{bmatrix}.$$

三个矩阵的秩都是 2，但是 $\mu(A)=1$，$\mu(B)=2$，而 $\mu(C)=3$. ◀

推论 4.116 设 C 是域 k 上的一个线性$[n, m]$-码，H 是 C 的一个奇偶性检验矩阵，则

(i) $d(C)=\mu(H)$.

(ii) $d(C)\leqslant m+1$.

证明 (i)设 $\beta_1, \cdots, \beta_n$ 是 H 的列向量. 因为 H 是 C 的奇偶性检验矩阵，字 $y=(y_1, \cdots, y_n)\in C$ 当且仅当 $yH^T=0$. 但 $yH^T=0$ 当且仅当 $Hy^T=0$，也就是，

$$y_1\beta_1+\cdots+y_n\beta_n=0.$$

设 $d(C)=d$，取权为 d 的码字 $y\in C$，设 y_{i_1}，…，y_{i_d}为 y 的非零坐标．因为 y 是一个非零的码字，所以

$$0=Hy^{\mathrm{T}}=y_1\beta_1+\cdots+y_n\beta_n=y_{i_1}\beta_{i_1}+\cdots+y_{i_d}\beta_{i_d},$$

故表 β_{i_1}，…，β_{i_d}是线性相关的，因此 $\mu(H)\leqslant d$．假设有线性相关的表 β_{j_1}，…，β_{j_p}，其中 $p<d$，则存在不全为零的纯量 z_{j_1}，…，z_{j_p} 使得 $z_{j_1}\beta_{j_1}+\cdots+z_{j_p}\beta_{j_p}=0$．定义 $\bar{z}=(\bar{z}_1,\cdots,\bar{z}_n)\in k^n$ 使得 $\bar{z}_{j_v}=z_{j_v}$，对 $v=1$，…，p，而其他的 $\bar{z}_j=0$，则 $H\bar{z}^{\mathrm{T}}=0$．因为 H 是 C 的一个奇偶性检验矩阵，则 $\bar{z}\in C$，这是一个矛盾，因为 $\mathrm{wt}(\bar{z})<d$．

413 (ii)由等式(2)，$\mu(H)\leqslant r+1$，其中 $\mathrm{rank}(H)=r$，因此 $r=m$． ■

→ **例 4.117** 在例 4.113 中，我们计算出汉明[7，4]-码 C 的最小距离为 3．应用在该例中给出的 C 的阶梯形生成矩阵，我们看到，C 的一个奇偶性检验矩阵是

$$H=\begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}$$

(因为元素在$\mathbb{B}=\mathbb{F}_2$ 中，我们有$-1=1$)．易见 H 的任意两列是线性无关的．因为第 1，4，5 列是线性相关的，因此 $\mu(H)=3$，所以 $d(C)=3$． ◀

现在我们希望能构造出能纠多个错且相对更有效的(线性)码．

回忆定理 3.114：若 k 是一个域，若 $f(x)\in k[x]$，$I=(f(x))$是由 $f(x)$生成的主理想，则商环 $k[x]/I$ 是 k 上的一个向量空间，有基为表 1，z，z^2，…，z^{n-1}，其中 $z=x+I$．因此 $k[x]/I$是 n 维的，且存在一个(向量空间的)同构 $k^n\to k[x]/I$．若我们记 k^n 中的字为$(a_0,a_1,\cdots,a_{n-1})$而不是$(a_1,\cdots,a_n)$，则$(a_0,a_1,\cdots,a_{n-1})\mapsto a_0+a_1z+\cdots+a_{n-1}z^{n-1}$是 $k^n\to k[x]/I$ 的一个同构．

→ **定义** 域上的长度为 n 的循环码是一个满足以下条件的线性码 C

$$(a_0,a_1,\cdots,a_{n-1})\in C\text{ 可推出}(a_{n-1},a_0,\cdots,a_{n-2})\in C.$$

$k[x]/I$ 是一个交换环，也是一个向量空间，这些事实现将被利用．请将以下证明与引理 3.26 的证明作比较．

→ **命题 4.118** 设 k 是一个有限域，$I=(x^n-1)$是 $k[x]$中由 x^n-1 生成的主理想．设 $z=x+I$，则 $C\subseteq k[x]/I$ 是一个循环码当且仅当 C 是交换环 $k[x]/I$ 中的一个理想．进一步，$C=(g(z))$，其中 $g(x)$是 $k[x]$中 x^n-1 的某首一因式．

证明 设 C 是 $k[x]/I$ 中的一个理想，$c=a_0+a_1z+\cdots+a_{n-1}z^{n-1}\in C$．因为 C 是一个理想，所以 C 包含 $zc=a_0z+a_1z^2+\cdots+a_{n-1}z^n$，但 $z^n=1$(因为 z 是 x^n-1 的一个根)．因此 $a_{n-1}+a_0z+a_1z^2+\cdots+a_{n-2}z^{n-1}\in C$，从而 C 是循环的．

相反地，假设 C 是一个循环码．因为 C 是一个线性码，所以 C 在加法下及在与 k 中元素的纯量乘法下是封闭的．像我们刚刚看到的一样，用 z 乘的结果是将函数向左边移进一步(并
414 且使得 a_{n-1}为常数项)．读者可以证明，对 i 进行归纳，C 在用所有元素 $b_0+b_1z+\cdots+b_{i-1}z^{i-1}\in k[x]/I$ 的乘积下是封闭的，因此 C 是一个理想．

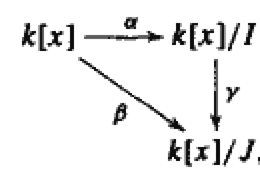
设 $\beta: k[x] \to k[x]/I$ 是自然映射，考虑逆象 $J=\beta^{-1}(C)=\{f(x)\in k[x]: f(z)\in C\}$. 由习题 3.47 知，$J$ 是 $k[x]$ 中包含 x^n-1 的一个理想. 但由定理 3.59，$k[x]$ 中每一个理想均为主理想，因此存在一个首一多项式 $g(x)\in k[x]$ 使得 $J=(g(x))$. 因为 $x^n-1\in J$，所以我们有 $x^n-1=h(x)g(x)$，对某多项式 $h(x)$，也就是 $g(x)\mid(x^n-1)$. 最后，因为 J 是由 $g(x)$ 生成，所以它的象 $C=\beta(J)$ 是由 $\beta(g(x))=g(z)$ 生成. ■

→ **定义** 设 $C\subseteq k[x]/I$ 是一个循环码，其中 $I=(x^n-1)$. 首一多项式 $g(x)\in k[x]$ 称为是 C 的一个**生成多项式**，若 $C=(g(z))$，其中 $z=x+I$.

与在命题 4.118 中一样，长度为 n 的一个循环码的生成多项式可选为 x^n-1 的一个因式，因此它的所有根都是 n 次单位根.

→ **推论 4.119** 若 C 是域 k 上一个长度为 n 的循环码，其一个生成多项式为 $g(x)$，则 $\dim(C)=n-\deg(g)$.

证明 因为 $g(x)\mid(x^n-1)$，所以存在理想间的包含关系 $I=(x^n-1)\subseteq(g(x))=J$. 视 $k[x]$ 和它的商仅仅为 k 上的向量空间，我们看到，由 $h(x)+I\mapsto h(x)+J$ 给出的“陪集的扩展”函数 $\gamma: k[x]/I\to k[x]/J$ 是一个满的线性变换. 为计算 $\ker\gamma$，考虑右图，其中 α，β 是自然映射. 注意 $\beta=\gamma\circ\alpha$，且 α，β 和 γ 都是满射，因此习题 2.102 的假设成立，所以



$$\ker\gamma=\alpha(\ker\beta)=\alpha((g(x))=(g(z))=C,$$

其中 $z=x+I$. 作为向量空间，$(k[x]/I)/C\cong k[x]/J$（这就是第一同构定理）. 因此

$$\dim(k[x]/I)-\dim(C)=\dim(k[x]/J).$$

但 $\dim(k[x]/I)=\deg(x^n-1)=n$ 且 $\dim(k[x]/J)=\dim(k[x]/(g(x)))=\deg(g)$，所以 $\dim(C)=n-\deg(g)$. ■ 415

推论 4.120 设 C 是一个长度为 n 的循环码，其生成多项式 $g(x)=g_0+g_1x+\cdots+g_sx^s$ 的次数 $\deg(g)=s$，则 C 的生成矩阵是下 $(n-s)\times n$ 的矩阵

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_s & 0 & 0 & \cdots & 0\\ 0 & g_0 & g_1 & g_2 & \cdots & g_s & 0 & \cdots & 0\\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_s & \cdots & 0\\ & & \vdots & & \vdots & & \vdots & & \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_s \end{bmatrix}.$$

证明 因为 C 是一个理想，所以 $g(x)$，$xg(x)$，…，$x^{n-s}g(x)$ 是码字，且这些码字对应于 G 的行. 记 $G=[X\mid T]$，其中 T 是由 G 的后 s 列构成的 $s\times s$ 的子矩阵. 因为 T 是一个对角线上元素全为 g_s 的下三角矩阵，由习题 4.51 我们有 $\det(T)=g_s^s$. 但 $g_s=1$，因为生成多项式是首一多项式. 因此 $\det(T)=1\neq 0$，从而 G 的 $n-s$ 行构成的表是线性无关的. 因为由推论 4.119，$\dim(C)=n-s$，所以 G 的行构成的表是 C 的一组基，从而 G 是 C 的一个生成矩阵. ■

→ **例 4.121** 设 C 是 $\mathbb{F}_7$ 上长度为 $n=6$ 的循环码，其生成多项式为

$$g(x)=(x-3)(x-3^2)(x-3^3)(x-3^4)=x^4+6x^3+3x^2+2x+4.$$

由推论 4.120，C 的一个生成矩阵是

$$N=\begin{bmatrix}4&2&3&6&1&0\\0&4&2&3&6&1\end{bmatrix}.$$

由高斯消元法，C 的一个阶梯形生成矩阵为

$$G=\begin{bmatrix}1&0&4&2&3&6\\0&1&4&6&5&2\end{bmatrix}.$$

一个奇偶性检验矩阵是

$$H=\begin{bmatrix}3&3&1&0&0&0\\5&1&0&1&0&0\\4&2&0&0&1&0\\1&5&0&0&0&1\end{bmatrix}.$$

读者可以验证 $GH^{\mathrm{T}}=0$. ◀

x^n-1 的根称为 n 次单位根. 回忆到域 k 中元素 z 称为 **n 次本质单位根**若 $z^n=1$ 且 $z^i\neq 1$，

416 对所有满足 $0<i<n$ 的 i.

引理 4.122 *设 $\mathbb{F}_q$ 表示有 q 个元素的有限域. 若 n 是一个正整数，则在 $\mathbb{F}_q$ 的某个扩域中存在一个 n 次本元单位根当且仅当 $\gcd(n, q)=1$.*

证明 假设 $(n, q)=1$，$E/\mathbb{F}_q$ 表示 $f(x)=x^n-1$ 的在 $\mathbb{F}_q$ 上的一个分裂域. 导数 $f'(x)=nx^{n-1}-1\neq 0$，所以 $\gcd(f, f')=1$（它们无相同的根），因此由习题 3.67 知，$f(x)$ 无重根. 从而，若 K 是 $f(x)=x^n-1$ 的所有根构成的集合，则 K 是一个 n 阶乘法群. 但由定理 3.55，K 是循环的，从而 K 的生成元一定是一个 n 次本原单位根.

相反地，假设存在一个 n 次本原单位根. 注意对某素数 p，$q=p^s$. 若 $(n, q)\neq 1$，则 $p\mid n$，也就是 $n=pu$，对某整数 u. 因此 $x^n-1=x^{pu}-1=(x^u-1)^p$，这样所有的 n 次单位根构成的乘法群的元素少于 n 个，从而无 n 次本原单位根. ■

→ **推论 4.123** *设 $C\subseteq\mathbb{F}_q^n$ 是一个循环码，其生成多项式是 $g(x)$，其中 $(n, q)=1$，则 $a=(a_0, a_1, \cdots, a_{n-1})\in\mathbb{F}_q^n$ 在 C 中当且仅当 $a(\eta)=0$，对 $g(x)$ 的每一根 η，其中 $a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$.*

证明 由命题 4.118，$C=(g)$，它是 $k[x]/I$ 中由 $g(x)+I$ 生成的主理想[其中 $I=(x^n-1)$]. 若 $a\in C$，则 $a\in(g)$，故存在 $f(x)\in k[x]$满足 $a(x)+I=f(x)g(x)+I$，因此 $a(x)-f(x)g(x)\in I$；存在某 $h(x)\in k[x]$使得

$$a(x)=f(x)g(x)+h(x)(x^n-1). \tag{3}$$

因为 $g(x)\mid(x^n-1)$，所以 $g(x)$ 的每个根均满足 $\eta^n=1$. 因为方程(3)右边是零，因此 $a(\eta)=0$.

因为 $(n, q)=1$，所以由引理 4.122 知 x^n-1 无重根. 因为 $g(x)\mid(x^n-1)$，所以生成多项式 $g(x)$ 也无重根. 从而当 η 取遍 $g(x)$ 所有根时，多项式 $x-\eta$ 是两两互素的. 若对 $g(x)$ 的每一个根 η 有 $a(\eta)=0$，则对每个 η，$x-\eta\mid a(x)$. 由习题 3.59 知，$a(x)$ 被 $\prod_{\eta}(x-\eta)=g(x)$ 整除，也就是 $a\in(g)=C$. ■

下面的定理将使得我们能够构造出能纠多个错且相对地更有效的码.

→ **定理 4.124(博泽-丘德贺理-霍可汉姆)**[⊖] 设 C 是 $\mathbb{F}_q$ 上长为 n 的一个循环码，其生成多项式为 $g(x)$，设 $(q, n)=1$，ζ 为一个 n 次单位原根. 若连续方幂 ζ^u，ζ^{u+1}，…，$\zeta^{u+\ell}$ 是 $g(x)$ 的根，其中 $0\leqslant u$ 且 $u+\ell<n$，则 $d=d(C)\geqslant\ell+2$.

证明 将码字 $c=(c_0, c_1, \cdots, c_{n-1})\in\mathbb{F}_q^n$ 与多项式 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in\mathbb{F}_q[x]$ 等同. 它的权数 $\mathrm{wt}(c)$ 是非零系数的个数. 由命题 4.110，只须证明每一个非零的码字至少有 417
$\ell+2$ 个非零的系数. 相反地，假设存在一个满足 $\mathrm{wt}(c)<\ell+2$ 的非零的码字 c. 因此 $c(x)=c_{i_1}x^{i_1}+\cdots+c_{i_{\ell+1}}x^{i_{\ell+1}}$，其中 $i_1<\cdots<i_{\ell+1}$. 若 $\beta\in\mathbb{F}_q$，则 $c(\beta)$ 是下点积：

$$c(\beta)=(c_{i_1},c_{i_2},\cdots,c_{i_{\ell+1}})\cdot(\beta^{i_1},\beta^{i_2},\cdots,\beta^{i_{\ell+1}}).$$

构造 $(\ell+1)\times(\ell+1)$ 的矩阵 W 使得它的第 j 列由 ζ^{u+j} 而得，对 $0\leqslant j\leqslant\ell$：

$$W=\begin{bmatrix}\zeta^{ui_1} & \zeta^{ui_2} & \cdots & \zeta^{ui_{\ell+1}}\\ \zeta^{(u+1)i_1} & \zeta^{(u+1)i_2} & \cdots & \zeta^{(u+1)i_{\ell+1}}\\ & \vdots & \vdots & \\ \zeta^{(u+\ell)i_1} & \zeta^{(u+\ell)i_2} & \cdots & \zeta^{(u+\ell)i_{\ell+1}}\end{bmatrix}$$

因此，若 $c_*=(c_{i_1}, \cdots, c_{i_{\ell+1}})$，则

$$Wc_*^{\mathrm{T}}=(c(\zeta^u),c(\zeta^{u+1}),\cdots,c(\zeta^{u+\ell}))^{\mathrm{T}}=0.$$

对所有 j，用 ζ^{ui_j} 去除 W 的第 j 列，即得到 $(\ell+1)\times(\ell+1)$ 的范德蒙德矩阵(的转置)：

$$V=\mathrm{Van}(\zeta^{i_1},\cdots,\zeta^{i_{\ell+1}})=\begin{bmatrix}1 & 1 & \cdots & 1\\ \zeta^{i_1} & \zeta^{i_2} & \cdots & \zeta^{i_{\ell+1}}\\ \zeta^{2i_1} & \zeta^{2i_2} & \cdots & \zeta^{2i_{\ell+1}}\\ & \vdots & \vdots & \\ \zeta^{\ell i_1} & \zeta^{\ell i_2} & \cdots & \zeta^{\ell i_{\ell+1}}\end{bmatrix}$$

由习题 4.52，我们有

$$\det(W)=\zeta^{ui_1}\cdots\zeta^{ui_\ell}\det(V)=\zeta^{ui_1}\cdots\zeta^{ui_\ell}\prod_{j<k}(\zeta^{i_k}-\zeta^{i_j}).$$

我们断言所有 ζ^{i_j} 是不同的. 若 $j<k$，则 $0\leqslant i_k-i_j<n$(因为 $i_j<i_k<n$)，所以 $\zeta^{i_k-i_j}=1$. 因此，若 $\zeta^{i_k}=\zeta^{i_j}$，则与 ζ 是 n 次本原单位根矛盾. 我们得出结论 $\det(W)\neq0$. 但 $c_*^{\mathrm{T}}\neq0$ 且 $Wc_*^{\mathrm{T}}=0$，这与 W 的非退化性矛盾，从而权 $<\ell+2$ 的码字不存在，即 $d(C)\geqslant\ell+2$. ■

为更明智地应用定理 4.124，我们对给定的 d 和 n 来寻求有效的码，这就是，我们想使信息率最大化，这就要使 $\deg(g)$ 极小化(因为由推论 4.119，$m=n-\deg(g)$). 418

→ **定义** 域 k 上的一个线性码称为是一个长度为 n 的 **BCH 码**，若它是一个具有最小可能次数的生成多项式 $g(x)$ 的循环码，且 $g(x)$ 的根中有连续方幂 ζ^u，ζ^{u+1}，…，$\zeta^{u+\ell}$，其中 ζ 是一个 n 次本原单位根，$0\leqslant u\leqslant u+\ell<n$.

→ **推论 4.125** 设 C 是一个长为 n 的 BCH 码，其生成多项式为 $g(x)$. 若连续方幂 ζ^u，ζ^{u+1}，…，ζ^{u+2t} 出现在 $g(x)$ 的根中，其中 $0\leqslant u$ 且 $u+2t<n$，则 C 可纠 t 个错. 进一步，设 y 是一个字，若满足 $\delta(y, c)\leqslant t$ 的码字 c 存在的话，则 c 一定唯一.

⊖ “博泽-丘德贺理-霍可汉姆”即 Bose-Chaudhuri-Hocquenghem. ——译者注

证明 用定理 4.124 的记号，我们有 $\ell=2t$，故由此定理，$d(C)\geqslant\ell+2\geqslant 2t+1$. 命题 4.108(iii)表明 C 可纠 t 个错. 命题 4.108(i)表明了满足 $\delta(y, c)\leqslant t$ 的码字 C 的唯一性，若有一个这样的 C 存在的话. ■

→ **推论 4.126** 对任意素数 p 和任意正整数 t，存在 $\mathbb{F}_p$ 上的一个可纠 t 个错的 BCH 码.

证明 设 $k=\mathbb{F}_q$，其中 q 是 p 的方幂，$2t+1<q-1$. 由定理 3.55，乘法群 $k^{\times}$ 是一个阶为 $q-1$ 的循环群，生成元 ζ 是一个 $q-1$ 次本原单位根. 因此 $\zeta, \zeta^2, \cdots, \zeta^{2t+1}$ 是不同的. 由命题 4.32，每一个 ζ^j 是 $\mathbb{F}_p[x]$ 中某多项式的根. 推论 3.117 给出了以 ζ^j 为一个根的唯一的首一不可约多项式 $h_j(x)\in\mathbb{F}_p[x]$. 最后，定义

$$g(x)=\operatorname{lcm}\{h_1(x),\cdots,h_{2t+1}(x)\},$$

定义 C 为以 $g(x)$ 为生成多项式的 BCH 码，由推论 4.125 即得出此结论. ■

没有一个简单的确定的能给出 BCH 码的生成多项式的次数的公式是已知的，但存在描述它们的大相关范围的表.

要判断以 $g(x)\in\mathbb{F}_q[x]$ 为生成多项式的一个循环码是否为一个 BCH 码，我们必须决定 $g(x)$ 的根，这就迫使我们更详细地研究有限域.

→ **例 4.127** 让我们来描述 $\mathbb{F}_8$. 我们知道，它的非零元构成的乘法群是 7 阶循环群，生成元是一个 7 次本原单位根. 存在一个以 ζ 为根的不可约多项式 $m(x)\in\mathbb{F}_2[x]$. 像在例题 3.116 中一样，$\deg(m)=3=\dim_{\mathbb{F}_2}(\mathbb{F}_8)$. 在例 3.98 中我们看到，在 $\mathbb{F}_2[x]$ 中，仅存在两个不可约三次多项式，即 x^3+x+1，x^3+x^2+1. 为更清楚些，我们首先选择 ζ 为第一个多项式的一个根，这样

表 4-1 是 $\mathbb{F}_8$ 的加法表. 因为 $\mathbb{F}_8$ 的特征为 2，所以对角线上的元素形如 $\zeta^i+\zeta^i=2\zeta^i=0$. 因
419 为加法是交换的，所以加法表是一个对称矩阵，因此只需要计算它的上三角部分. 让我们计算

$$\zeta^3=\zeta+1.$$

表 4-1 $\mathbb{F}_8$ 的加法表

+	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6
1	0	ζ^3	ζ^6	ζ	ζ^5	ζ^4	ζ^2
ζ		0	ζ^4	1	ζ^3	ζ^6	ζ^5
ζ^2			0	ζ^5	ζ	ζ^3	1
ζ^3				0	ζ^6	ζ^2	ζ^4
ζ^4					0	1	ζ^3
ζ^5						0	ζ
ζ^6							0

表 4-1中的第一行，它由 ζ^j+1 构成，其中 $1\leqslant j\leqslant 6$. 我们有 $\zeta+1=\zeta^3$ 且 $\zeta^3+1=(\zeta+1)+1=\zeta$. 其次

$$\zeta^2+1=(\zeta+1)^2=(\zeta^3)^2=\zeta^6;$$
$$\zeta^4+1=(\zeta^2+1)^2=(\zeta^6)^2=\zeta^{12}=\zeta^5;$$

$$\zeta^6+1=(\zeta^3+1)^2=\zeta^2.$$

由此得出 $\zeta^5+1=\zeta^4$，因为 ζ 的其他的方幂都已经出现了．现在我们来用第一行来计算第二行．例如，$\zeta^j+\zeta=\zeta(\zeta^{j-1}+1)$，请读者验证其余的项． ◀

→ **例 4.128** (i)在 $\mathbb{F}_2[x]$ 中，x^7-1 的不可约多项式分解是

$$x^7-1=x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1).$$

设 C 是长为 7 的循环二元码，其生成多项式为 $g(x)=x^3+x+1$．注意 $g(x)$ 有一个根是一个 7 次本原单位根，记为 ζ．为求其他的根，我们来应用表 4-1．对每一个 i，求 $f(\zeta^i)$ 的值．我们看到 ζ 和 ζ^2 的连续根，因此 C 是一个 BCH 码，相应的 $\ell=1$．事实上，C 是一个[7，4]-码．[因为 $7-\deg(g)=4$]，且 $d(C)\geqslant\ell+2=3$．由推论 4.120，C 的一个生成矩阵是

$$G=\begin{bmatrix}1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}.$$ 420

G 的阶梯形是

$$G'=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}.$$

因此，C 是例 4.113 中的汉明[7，4]-码，所以此码是一个 BCH 码(可以证明，所有汉明码都是 BCH 码)．

(ii)考虑具有如下生成多项式的长为 7 的循环二元码 C，

$$g(x)=(x+1)(x^3+x+1)=x^4+x^3+x^2+1.$$

注意 $1=\zeta^0$，ζ 和 ζ^2 是 $g(x)$ 的根，所以 C 是一个 BCH 码．事实上，C 是一个[7，3]-码，且 $d(C)\geqslant 4$．由推论 4.120，C 的一个生成矩阵是

$$G=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\end{bmatrix}.$$ ◀

通过应用有限域 $\mathbb{F}_q$ 而不是素域 $\mathbb{F}_p$，我们可以选择多项式，使得它比一般的 BCH 码的生成多项式更简单．

→ **推论 4.129(理德-索罗门)** *设 q 是一个素数幂，t 是一个正整数，且满足 $2t\leqslant q-1$．则存在 $\mathbb{F}_q$ 上长为 $q-1$ 的一个码，它可纠 t 个错且它的信息率为 $1-\dfrac{2t}{q-1}$．*

证明 设 $\zeta\in\mathbb{F}_q$ 为一个 $q-1$ 次本原单位根．设

$$g(x)=(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{2t})\in\mathbb{F}_q[x],$$

其中 $2t<q-1$．设 $C\subseteq\mathbb{F}_q^{q-1}$ 为一个生成多项式为 $g(x)$ 的码．使用定理 4.124 的记号，$1+\ell=2t$，故定理 4.124 推出 $d(C)\geqslant\ell+2=2t+1$．由命题 4.108(iii)知，码 C 可纠 t 个错．因为

$\deg(g)=2t$，所以由推论 4.119，$\dim(C)=q-1-2t$. 因此，C 的信息率是 $\frac{q-1-2t}{q-1}=1-\frac{2t}{q-1}$. ■

→ **定义** $\mathbb{F}_q$ **上一个纠 t 个错的理德-索罗门(Reed-Solomon)码**指的是一个长为 $q-1$ 的 BCH 码，且其生成多项式为

$$g(x)=(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{2t}),$$

其中 ζ 是 $\mathbb{F}_q$ 中一个 $q-1$ 次本原单位根且 $2t<q-1$.

我们说过不存在计算一般 BCH 码的生成多项式的次数的简单公式. 相对地，在推论 4.129 中，生成多项式的次数是 $2t$. 若 C 是一个纠 t 个错的理德-索罗门码，则由推论 4.129

421 知，$\dim(C)=q-1-2t$.

→ **例 4.130** 在 $\mathbb{F}_7$ 中 $[3]$ 是一个 6 次本原单位根. 以多项式

$$g(x)=(x-3)(x-3^2)(x-3^3)(x-3^4)=4+2x+3x^2+6x^3+x^4$$

为生成多项式的码 C 是 $\mathbb{F}_7$ 上的一个纠 2 个错的理德-索罗门码. 由例 4.121，C 的一个生成矩阵是

$$G=\begin{bmatrix}4 & 2 & 3 & 6 & 1 & 0\\ 0 & 4 & 2 & 3 & 6 & 1\end{bmatrix}.$$

因此 C 是行空间 $Row(G)$：

$$C=\{(4a,2a+4b,3a+2b,6a+3b,a+6b,b):a,b\in\mathbb{F}_7\}.$$ ◀

→ **例 4.131** 设 $\zeta\in\mathbb{F}_8$ 是一个 7 次本原单位根. 以多项式

$$g(x)=(x+\zeta)(x+\zeta^2)(x+\zeta^3)(x+\zeta^4)$$

为生成多项式的 $\mathbb{F}_8$ 上的 BCH[7，3]码是一个 $\mathbb{F}_8$ 上的纠 2 个错的理德-索罗门码(因为 $\mathbb{F}_8$ 的特征为 2，所以 $-1=1$). 应用表 4-1，我们看到 $g(x)=\zeta^3+\zeta x+x^2+\zeta^3x^3+x^4$. 由推论 4.120，$C$ 的一个生成矩阵是

$$G=\begin{bmatrix}\zeta^3 & \zeta & 1 & \zeta^3 & 1 & 0 & 0\\ 0 & \zeta^3 & \zeta & 1 & \zeta^3 & 1 & 0\\ 0 & 0 & \zeta^3 & \zeta & 1 & \zeta^3 & 1\end{bmatrix}.$$ ◀

从太空发送来的一个长信息有可能被一个宇宙射线击中而导致破裂，即把一串连续的字母搞乱. 为对付破裂，人们首先应用 $\mathbb{F}_8$ 上的一个理德-索罗门码对信息进行编码，其中 q 是 2 的方幂. 例如，设 C 是 $\mathbb{F}_{256}$ 上的纠 5 个错的理德-索罗门码，其生成多项式为 $g(x)=\prod_{i=1}^{10}(x-\zeta^i)$，其中 ζ 是一个 255 次本原单位根. 注意因为 $256=2^8$，所以 $\mathbb{F}_{256}$ 中每个元素都可以写成长为 8 的一个串. 通过将 C 中的码字中的(属于 $\mathbb{F}_{256}$ 中的)字母替换成长为 8 的串来构造一个长为 $8\cdot255=2040$ 的二进制代码 C'. 用二进制代码 C' 发送一个信息，并且译码成理德-索罗门码 C. 因为 C 可纠 5 个错，因此在收到的二进制信息中，这对应于可改正一个长度为 33 个二进制符号的二进制区间(一个长度为 34 的区间涉及理德-索罗门码的 6 个字母). 按这种方式，理德-索罗门

422 码可应用有限域的理论来改正二进制的错误的破裂.

4.5.3 译码

设$\mathcal{A}$是一个有限字母表，$C\subseteq\mathcal{A}^n$是一个$[n, m]$块码. 一个字 $y\in\mathcal{A}^n$可按下面效率低的方式进行译码. 将所有的字 $c\in C$ 进行编号，如，c_1，…，c_r，其中 $r=|\mathcal{A}|^m$. 对所有 i 计算 $\delta(y, c_i)$. 译码 y 为 c_i，其中 c_i 是距 y 最近的码字(若存在数个最近的码字，取编号在最前的码字).

若 $C\subseteq\mathbb{F}_q^n$是一个线性码，则刚刚描述的朴素的译码方式可更好地组织. 但它仍然是效率低下的. 我们的目标是将按收到的字 y 译码成与之最近码字 c，这就启发我们去考虑形如 $y-c$(其中 $c\in C$)的字，因为 $\delta(y, c)=\mathrm{wt}(y-c)$.

→ **定义** 设 $C\subseteq\mathbb{F}_q^n$是一线性$[n, m]$码. 若 $y\in\mathbb{F}_q^n$且$c\in C$，则**错误向量**指的是 $e=e(y, c)=y-c$.

注意向量空间$\mathbb{F}_q^n$是一个加法交换群，C 是一个子群. 给定 y，则所有错误向量 $y-c$ 的总体就是陪集 $y+C$，$c\in C$. 说 $c\in C$ 是与 y 最近的码字就是说错误向量 $e(y, c)=y-c$ 在 $y+C$ 中是权最小的.

定义 若 $C\subseteq\mathbb{F}_q^n$是一线性$[n, m]$码. 若 $y+C$ 是 C 在$\mathbb{F}_q^n$中的一个陪集，则一个**陪集的头字**指的是一个权最小的向量 $e\in y+C$.

$\mathbb{F}_q^n$中的向量可以适当组织使得一个分组码的朴素的译码方式变得稍为更有效些. 将所有字 $c\in C$ 进行编号，如，c_1，…，c_{q^m}，对一组陪集代表元再进行编号，如，w_1，…，$w_{q^{n-m}}$. 作一个表使得它的第 j 列由第 j 个陪集 $w_j+C=\{w_j+c_i: i=1, \cdots, q^m\}$的元素排列而成. 给定一个向量 y，确定它所在的(唯一的)列 w_j+C(群$\mathbb{F}_q^n$是所有不交的陪集的并). 若 e_j 是一个陪集的头字，则 $e_j=y-c$，对某 $c\in C$，从而 c 是一个与 y 最近的字. (如果最近的字多于一个，则在陪集 w_j+C 的列举中选择第一个). 我们可以使得此程序的效率变得稍微高一些. 若 H 是 C 的一个检验矩阵，则由例题 4.114，$y\in C$ 当且仅当 $yH^T=0$. 而两个向量 y，$w\in\mathbb{F}_q^n$属于 C 的同一个陪集当且仅当$y-w=c\in C$. 但 $yH^T-wH^T=(y-w)H^T=cH^T=0$，因此 y，$w\in\mathbb{F}_q^n$在 C 的同一个陪集中当且仅当$yH^T=wH^T$.

→ **定义** 设 H 是一个线性$[n, m]$-码 $C\subseteq\mathbb{F}_q^n$的检验矩阵. 若 $y\in\mathbb{F}_q^n$，则它的**和声**指的是 $S(y)=yH^T$.

线性码 C 的检验矩阵 H 不必是唯一的，而和声 yH^T 的确依赖于 H 的选取. 为对一个收到的字 y 进行译码，首先计算它的和声 $S(y)=yH^T$，接着计算陪集的头字 e_j 的和声 $S(y)=yH^T$，直 423
至 $S(e_j)=S(y)$ 成立. 只有一个这样的陪集 e_j+C 存在，因为若 $S(e_j)=S(e_k)$，则 $S(e_j-e_k)=0$，$e_j-e_k\in C$，从而 $e_j+C=e_k+C$. 因此$c=y-e_j$ 是与 y 最近的码字，即 y 被译成 c. 尽管此方法比一般分组码的朴素译码方式好一些，但它仍然不是很实用的. 总之，若 C 是 $\mathbb{F}_q$ 上的一个$[n, m]$线性码，则 C 有 q^{n-m}个陪集.

对所有 BCH 码，存在效率高的译码程序. 但我们将精力集中在理德-索罗门码上. 更精确地，若 C 是一个$\mathbb{F}_q$ 上的纠 t 个错的理德-索罗门码. 对某码字 c，若 y 是满足$\delta(y, c)\leqslant t$ 的一个接收到的字，则我们将说明如何去求 c(没有更多的信息，试图去译一个与任一个码字都不靠近的字是非常愚蠢的).

通常，我们将一个向量 $y=(y_0, y_1, \cdots, y_{q-2})\in\mathbb{F}_q^{q-1}$看成一个多项式 $y(x)=y_0+y_1x$

$+\cdots+y_{q-2}x^{q-2}\in \mathbf{F}_q[x]$.

→ **命题 4.132** 设 ζ 是 $\mathbf{F}_q$ 的一个本原元素，$C\subseteq \mathbf{F}_q^{q-1}$ 是 $\mathbf{F}_q$ 上的一个纠 t 个错的理德-索罗门码，其生成多项式 $g(x)=(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{2t})$. 定义 $2t\times(q-1)$ 的矩阵

$$U=\begin{bmatrix}1 & \zeta & \zeta^2 & \cdots & \zeta^{q-2}\\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(q-2)}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & \zeta^{2t} & \zeta^{4t} & \cdots & \zeta^{2t(q-2)}\end{bmatrix}$$

(i) 若 $y=(y_0, y_1, \cdots, y_{q-2})\in \mathbf{F}_q^{q-1}$，则

$$yU^T=(y(\zeta),y(\zeta^2),\cdots,y(\zeta^{2t})),$$

其中 $y(\zeta^i)=y_0+y_1\zeta^i+\cdots+y_{q-2}\zeta^{i(q-2)}$.

(ii) 设 $f(x)=f_0+f_1x+\cdots+f_rx^r\in \mathbf{F}_q[x]$，其中 $r\leqslant t$. 若我们记 $f=(f_0, \cdots, f_r, 0, \cdots, 0)\in \mathbf{F}_q^{2t}$，则

$$fU=(f(1),\zeta f(\zeta),\zeta^2 f(\zeta^2),\cdots,\zeta^{q-2}f(\zeta^{q-2})).$$

(iii) U 是 C 的一个检验矩阵.

(iv) 若 $e=y-c$ 是一个错误向量，则 e 和 y 有相同的和声：

$$S(e)=eU^T=yU^T=S(y),$$

424 因此对所有的 $j\leqslant 2t$，$e(\zeta^j)=y(\zeta^j)$.

证明 (i) 注意到 U 是 $\mathbf{F}_q$ 上的一个矩阵因为 $\zeta\in \mathbf{F}_q$(若 C 仅是一个 BCH 码，则这点未必成立). yU^T 的 ij 位元素是点积

$$y\cdot \mathrm{ROW}_U(i)=y_0+y_1\zeta^i+\cdots+y_{q-2}\zeta^{i(q-2)}=y(\zeta^i).$$

因此

$$yU^T=(y(\zeta),y(\zeta^2),\cdots,y(\zeta^{2t})).$$

(ii) fU 的 ij 位元素是点积

$$\begin{aligned}(f_0,\cdots,f_r,0,\cdots,0)\cdot \mathrm{COL}_U(j)&=(f_0,\cdots,f_r,0,\cdots,0)\cdot(\zeta^j,\zeta^{2j},\cdots,\zeta^{2jt})\\ &=f_0\zeta^j+f_1\zeta^{2j}+\cdots+f_r\zeta^{2jr}\\ &=\zeta^j(f_0+f_1\zeta^j+\cdots+f_r\zeta^{jr})\\ &=\zeta^j f(\zeta^j).\end{aligned}$$

(iii) 由推论 4.123，若 $C\subseteq \mathbf{F}_q^{q-1}$ 是一个以 $g(x)$ 为生成多项式的循环码，则 $y=(y_0, y_1, \cdots, y_{q-2})\in \mathbf{F}_q^{q-1}$ 落在 C 中当且仅当 $y(\eta)=0$，对 $g(x)$ 的每一个根 η. 因此，$y\in C$ 当且仅当 $yU^T=0$.

(iv)

$$eU^T=(y-c)U^T=yU^T-cU^T=yU^T.$$

最后一个论断成立是因为 $yU^T=(y(\zeta), y(\zeta^2), \cdots, y(\zeta^{2t}))$. ■

设 C 是 $\mathbf{F}_q$ 上的一个纠 t 个错的理德-索罗门码. U 是例题 4.132 中的检验矩阵. 通过求 y 的错误向量 $e=y-c$ 来译接收到的字 y. 在译码过程中最困难的一步是确定 e 的非零坐标的位置. 总之，若 C 是一个二进制码，则 e 的非零坐标实际上是决定了 e(当然，一个理德-索罗门码 $C\subseteq \mathbf{F}_q^{q-1}$ 一定不是一个二进制码，除非 $q=2$ 且 $q-1=1$).

回忆第 3 章中的定义：若 $A=[a_{ij}]$和 $B=[b_{ij}]$是域 k 上的 $m\times n$ 的矩阵，则它们的**阿达马积**是 $A\circ B=[a_{ij}b_{ij}]$，特别地，$1\times n$ 的向量的阿达马积被定义为

$$[a_1,\cdots,a_n]\circ[b_1,\cdots,b_n]=[a_1b_1,\cdots,a_nb_n].$$

定义 若 e 是一个错误向量，则满足 $e\circ u=0$ 的非零向量 u 称为**错误定位向量**.

e 的支撑总是包含于一个错误定位向量 u 的零集中的. 425

引理 4.133 若 $e=(e_0,\cdots,e_{q-2})$和 $u=(u_0,\cdots,u_{q-2})$落在$\mathbb{F}_q^{q-1}$中，则由 $e\circ u=(0,\cdots,0)$可推出

$$\{j:e_j\neq 0\}=\mathrm{Supp}(e)\subseteq \mathcal{Z}(u)=\{j:u_j=0\}.$$

证明 假设 $e\circ u=(0,\cdots,0)$是说对所有的 j 有 $e_ju_j=0$. 若 $j\in\mathrm{Supp}(e)$，则 $e_j\neq 0$. 因为 $e_ju_j=0$，所以我们必有 $u_j=0$，从而 $j\in\mathcal{Z}(u)$. ■

我们来构造一个多项式，使得它的根以方幂 ζ^{j_v}的方式出现，其中 $j_v\in\mathrm{Supp}(e)$.

→ **定义** 设 C 是$\mathbb{F}_q$ 上的一个纠 t 个错的理德-索罗门码. 设 y 是一个接收到的字. 设 $e=y-c=(e_0,e_1,\cdots,e_{q-2})$是一个错误向量，若 $\mathrm{wt}(e)\leqslant t$ 且 $\mathrm{Supp}(e)=\{j_1,\cdots,j_r\}$，其中 $r\leqslant t$. 则**错误定位多项式**指的是

$$f(x)=(x-\zeta^{j_1})(x-\zeta^{j_2})\cdots(x-\zeta^{j_r})=f_0+f_1x+\cdots+f_{r-1}x^{r-1}+f_rx^r,$$

其中 $f_r=1$. 我们记 $f=(f_0,f_1,\cdots,f_{r-1},1,0,\cdots,0)\in\mathbb{F}_q^{2t}$(这样矩阵乘积 fU 就被定义了，其中 U 是命题 4.132 中的检验性矩阵).

现在我们来改进引理 4.133.

→ **引理 4.134** 设 C 是$\mathbb{F}_q$ 上的一个纠 t 个错的理德-索罗门码，设 U 是命题 4.132 中的检验性矩阵，设 y 是一个接收到的一个字，$e=y-c=(e_0,e_1,\cdots,e_{q-2})$是一个满足 $\mathrm{wt}(e)\leqslant t$ 的错误向量，若 $u=fU=(f(1),\zeta f(\zeta),\cdots,\zeta^{q-2}f(\zeta^{q-2}))$，其中 $f=(f_0,f_1,\cdots,f_{r-1},1,0,\cdots,0)\in\mathbb{F}_q^{2t}$是错误定位多项式，则 U 是一个错误定位向量且

$$\mathrm{Supp}(e)=\mathcal{Z}(u).$$

证明 设 $\mathrm{Supp}(e)=\{j_1,\cdots,j_r\}$，其中 $r\leqslant t$. 设 $f(x)=\sum_{i=1}^{r}f_ix^i$ 为错误定位多项式，我们断言 $e\circ u=0$. 若 $j_v\in\mathrm{Supp}(e)$，则由命题 4.132(ii)，$u_{j_v}=f(\zeta^{j_v})=0$，所以 $e_{j_v}u_{j_v}=0$. 若 $j\notin\mathrm{Supp}(e)$，则 $e_j=0$. 所以 $e_ju_j=0$，因此 $e\circ u=[0,\cdots,0]$. 也就是 u 是一个错误定位向量. 由引理 4.133 得出 $\mathrm{Supp}(e)\subseteq\mathcal{Z}(u)$. 此包含关系不可能是真包含：若 $u_j=0$，对某 $j\notin\{j_1,\cdots,j_r\}$，则 $\zeta^jf(\zeta^j)=0$，因此 $f(\zeta^j)=0$，它给出了次数 $r\leqslant t$ 的多项式 $f(x)$的太多的根，因此 $\mathrm{Supp}(e)=\mathcal{Z}(u)$. ■

我们现在来证明错误定位多项式，且错误定位向量可以通过求解一个线性方程组而求得.

定义 设 C 是$\mathbb{F}_q$ 上的一个纠 t 个错的理德-索罗门码，设 ζ 为$\mathbb{F}_q$ 的一个本原根，$y=(y_0,y_1,\cdots,y_{q-2})\in\mathbb{F}_q^{q-1}$，$e=y-c$ 是一个满足 $\mathrm{wt}(e)=r\leqslant t$ 的错误向量. 则**和声矩阵**指的是 $r\times r$ 的矩阵 426

$$\Sigma(y)=\begin{bmatrix}y(\zeta) & y(\zeta^2) & \cdots & y(\zeta^r)\\ y(\zeta^2) & y(\zeta^3) & \cdots & y(\zeta^{r+1})\\ \vdots & \vdots & \cdots & \vdots\\ y(\zeta^r) & y(\zeta^{r+1}) & \cdots & y(\zeta^{2r-1})\end{bmatrix}$$

→ **命题 4.135** 设 C 是 $\mathbb{F}_q$ 上的一个纠 t 个错的理德-索罗门码，$y=(y_0, y_1, \cdots, y_{q-2})\in \mathbb{F}_q^{q-1}$，$e=y-c$ 是一个满足 $\mathrm{wt}(e)=r\leqslant t$ 的错误向量.

(i) e 和 y 有相同的和声矩阵：$\Sigma(e)=\Sigma(y)$.

(ii) 若 $f(x)=f_0+f_1x+\cdots+f_{r-1}x^{r-1}+x^r$ 是错误多项式，则

$$\dot{f}=(f_0, f_1, \cdots, f_{r-1})\in \mathbb{F}_q^r$$

是线性方程组

$$\Sigma(y)\dot{f}^T=h^T$$

的一个解，其中 $h=[-y(\zeta^{r+1}), -y(\zeta^{r+2}), \cdots, -y(\zeta^{2r})]$.

(iii) 和声矩阵 $\Sigma(y)$ 是非奇异的.

证明 (i) 由命题 4.132(iv) 知 e 和 y 有相同的和声，又由命题 4.132(ii)，对所有的 $j<2t$，我们有 $e(\zeta^j)=y(\zeta^j)$，因此 $\Sigma(e)=\Sigma(y)$.

(ii) 对 $v=1, \cdots, r$，每一个 ζ^{j_v} 是错误定位多项式 $f(x)$ 的一个根，所以

$$f_0+f_1\zeta^{j_v}+f_2\zeta^{2j_v}+\cdots+f_{r-1}\zeta^{(r-1)j_v}+\zeta^{rj_v}=0.$$

对每一个 $i=1, \cdots, r$，用 ζ^{ij_v} 乘此方程可得

$$f_0\zeta^{ij_v}+f_1\zeta^{(i+1)j_v}+\cdots+f_{r-1}\zeta^{(i+r-1)j_v}+\zeta^{(i+r)j_v}=0.$$

回忆到 $e(x)=e_{j_1}x^{j_1}+e_{j_2}x^{j_2}+\cdots+e_{j_r}x^{j_r}$，将 $v=1, \cdots, r$ 的方程连加，即得到

$$f_0e(\zeta^i)+f_1e(\zeta^{i+1})+\cdots+f_{r-1}e(\zeta^{i+r-1})+\zeta^{i+r}=0.$$

因此，对 $i=1, \cdots, r$，这 r 个方程构成一个非奇次 $r\times r$ 的线性方程组

$$\Sigma(e)\dot{f}^T=h^T,$$

427 其中 $h=[-y(\zeta^{r+1}), -y(\zeta^{r+2}), \cdots, -y(\zeta^{2r})]^T$. 但是由 (i) 有 $\Sigma(e)=\Sigma(y)$.

(iii) 我们断言存在分解 $\Sigma(y)=VDV^T$，其中 V 是 $r\times r$ 的范得蒙德矩阵

$$V=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \zeta^{j_1} & \zeta^{j_2} & \cdots & \zeta^{j_r} \\ \zeta^{2j_1} & \zeta^{2j_2} & \cdots & \zeta^{2j_r} \\ \vdots & \vdots & \cdots & \vdots \\ \zeta^{(r-1)j_1} & \zeta^{(r-1)j_2} & \cdots & \zeta^{(r-1)j_r} \end{bmatrix}$$

且 $D=\mathrm{diag}\{e_{j_1}\zeta^{j_1}, e_{j_2}\zeta^{j_2}, \cdots, e_{j_r}\zeta^{j_r}\}$. 注意矩阵 VD 是用 $e_{j_v}\zeta^{j_v}$ 乘 V 的第 v 列而得到的. 对所有的 $v=1, \cdots, r$，考虑乘积

$$(V\,D)V^T=\begin{bmatrix} e_{j_1}\zeta^{j_1} & e_{j_2}\zeta^{j_2} & \cdots & e_{j_r}\zeta^{j_r} \\ e_{j_1}\zeta^{2j_1} & e_{j_2}\zeta^{2j_2} & \cdots & e_{j_r}\zeta^{2j_r} \\ \vdots & \vdots & \cdots & \vdots \\ e_{j_1}\zeta^{rj_1} & e_{j_2}\zeta^{rj_2} & \cdots & e_{j_r}\zeta^{rj_r} \end{bmatrix}\begin{bmatrix} 1 & \zeta^{j_1} & \cdots & \zeta^{rj_1} \\ 1 & \zeta^{j_2} & \cdots & \zeta^{rj_2} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \zeta^{j_r} & \cdots & \zeta^{rj_r} \end{bmatrix}$$

则 $(VD)V^T$ 的 (1, 1) 位元素是

$$e_{j_1}\zeta^{j_1}+e_{j_2}\zeta^{j_2}+\cdots+e_{j_r}\zeta^{j_r}=e(\zeta).$$

事实上，应用命题 4.132(iv)，类似的计算表明 VDV^T 所有的元素与 $\Sigma(y)$ 相应的元素相等.

因为所有 ζ^{j_ν} 是不同的，所以由习题 4.52，范得蒙德矩阵 V 是非奇异的. 对角矩阵 D 是非奇异的因为它的对角线元素都是非零的. 因此 $\Sigma(y)=VDV^T$ 是非奇异的. ■

命题 4.135 可求出错误向量 e 的错误位置 j_1，…，j_r. 通过解线性方程组 $\Sigma(y)\dot{f}^T=h^T$ 可求出错误定位多项式 $f(x)$[$\dot{f}$ 的唯一性由 $\Sigma(y)$ 的非奇异性而得]. 因为 $\dot{f}=(f_0, f_1, \cdots, f_{r-1})$，所以我们有 $f(x)=f_0+f_1x+\cdots+f_{r-1}x^{r-1}+x^r$. 首一多项式 $f(x)$ 确定错误定位向量 $u=fU$，其中 U 是命题 4.132 中的检验矩阵，引理 4.134 给出 $\{j_1, \cdots, j_r\}=\mathrm{Supp}(e)=\mathcal{Z}(u)$. 要译码 y，我们去掉元素 y_{j_1}，…，y_{j_r}，将这些错误的元素替换成真实的值.

下定理是译理德-索罗门码的方法，推广此方法可译所有的 BCH 码.

→ **定理 4.136** *设 C 是 $\mathbb{F}_q$ 上的一个纠 t 个错的理德-索罗门码，y 是一个字，存在一个满足 $\mathrm{wt}(e)\leqslant t$ 的错误向量 e，则 y 可以被有效地译码.*

证明 命题 4.135 可求出错误向量 e 中的错误位置 j_1，…，j_r，因为 $\mathrm{Supp}(e)=\mathcal{Z}(fU)$，其中 $f(x)$ 是错误定位多项式，U 是命题 4.132 中 C 的检验矩阵. 428

首先设 $r=t$. 设 U^* 是在 U 中去掉除第 j_1，…，j_r 行外的其他行而得的矩阵. 由习题 4.31，通过解 $U^*e^*=Uy^T$，可以求出 e 的非零坐标[按我们用下面的记号，e^* 是 $1\times t$ 的向量 $(e_{j_1}, \cdots, e_{j_t})$. 习题 4.31 进一步说此更小的非奇次线性方程是可解的(用高斯消元法)若 $\mathrm{rank}(U^*)=t$. 此时是这样的，U 的任意 t 行构成一个非奇异的 $t\times t$ 的范德蒙德矩阵，因为它的行是不同的，所以任意 t 行构成一个线性无关的表. 求出了 e^*，从而求出 e，我们就有码字 $c=y-e$. 由推论 4.125，c 是唯一的与 y 最近的码字. 译码 y 为 $E^{-1}(c)$，其中 E 是编码函数.

若 $r<t$，则此程序将失效[和声矩阵 $\Sigma(y)$ 为奇异的，错误定位多项式就不可能确定]. 求出使得 $r\times r$ 的矩阵 $\Sigma(y)$ 是非奇异的最大的 $r\leqslant t$，则结束译码. ■

→ **例 4.137** 设 C 是例 4.130 给出的 $\mathbb{F}_7$ 上的一个纠 2 个错的理德-索罗门码，注意 3 是 $\mathbb{F}_7$ 中 6 次本原单位根：

$$3^2=9\equiv 2,\quad 3^3=27\equiv 6,\quad 3^4=81\equiv 4,\quad 3^5=243\equiv 5,\quad 3^6\equiv 1.$$

这里 $t=2$，$q=7$，因此命题 4.132 中的检验性矩阵 U 是下面的 4×7 的矩阵

$$U=\begin{bmatrix}1&3&2&6&4&5\\1&2&4&1&2&4\\1&6&1&6&1&6\\1&4&2&1&4&2\end{bmatrix}.$$

假设存在一个满足 $\mathrm{wt}(e)\leqslant 2$ 的错误向量 e，我们来译字 $y=(4, 0, 5, 1, 0, 1)$.

(i) 和声是 $yU^T=S(y)=(4, 1, 0, 3)$.

(ii) 和声矩阵是 $\Sigma(y)=\begin{bmatrix}4&1\\1&0\end{bmatrix}$.

(iii) 解 $\Sigma(y)\dot{f}^T=h^T$，此时为 $\begin{bmatrix}4&1\\1&0\end{bmatrix}\begin{bmatrix}f_0\\f_1\end{bmatrix}=\begin{bmatrix}4\\5\end{bmatrix}$，得到 $\dot{f}=(4, 5)$. 因此错误定位多项式

是 $f(x)=4+5x+x^2$.

(iv)错误定位向量是 $u=fU=(3, 0, 1, 0, 6, 4)$. 因此 $\mathcal{Z}(u)=\{1, 3\}$，故 $\operatorname{Supp}(e)=\{1, 3\}$.

(v)求解方程组 $U^* e^* = Uy^T$，此时为

429

$$\begin{bmatrix}3 & 6\\2 & 1\\6 & 6\\4 & 1\end{bmatrix}\begin{bmatrix}e_1\\e_3\end{bmatrix}=\begin{bmatrix}4\\1\\0\\3\end{bmatrix}.$$

解为 $e^*=(1, 6)$. 错误向量是 $e=(0, 1, 0, 6, 0, 0)$. 我们现在来译 y.

$$\begin{aligned}c &= y-e\\&=(4,0,5,1,0,1)-(0,1,0,6,0,0)\\&=(4,-6,5,2,0,1)\\&=(4,1,5,2,0,1)\end{aligned}$$

因此 y 被译成 $E^{-1}(c)$，其中 E 是编码函数. ■

习题

4.66 设$\mathcal{A}$是一个字母表，$|\mathcal{A}|=q\geqslant 2$，设 $T: \mathcal{A}^n\to\mathcal{A}^n$ 为一个发送函数. 设发送字时一个字母出错的概率为 p，其中 $0<p<1$.

(i)试证在发送一个字母长为 n 的字的时候，恰好出现 ℓ 个错字母的事件的概率是 $P=\left(\frac{p}{p-1}\right)^\ell(1-p)^{n-\ell}$.

(ii)试证 $P=\binom{n}{\ell}p^\ell(1-p)^{n-\ell}$，由此得出结论概率 P 是与 q 无关的.

* 4.67 试证 $d\geqslant 3$，其中 d 是例 4.105(iii)中二维奇偶性码的最小矩离.

* 4.68 设$\mathcal{A}$是一个字母表，$|\mathcal{A}|=q$，设 $C\subseteq\mathcal{A}^n$是一个(n, M, d)-码.

(i)定义 $\pi: C\to\mathcal{A}^{n-d+1}$ 为 $\pi(c_1, \cdots, c_n)=(c_d, \cdots, c_n)$. 试证 π 是一个单射.

(ii)(**单字界**)试证

$$M\leqslant q^{n-d+1}.$$

* 4.69 设$\mathcal{A}$是一个字母表，$|\mathcal{A}|=q$. 若 $u\in\mathcal{A}^n$，定义以 u 为中心的以 r 为半径(闭)的球为

$$B_r(u)=\{w\in\mathcal{A}^n: \delta(w,u)\leqslant r\},$$

其中 δ 是汉明距离.

(i)试证

$$|\{w\in\mathcal{A}^n: \delta(u,w)=i\}|=\binom{n}{i}(q-1)^i.$$

(ii)试证

430

$$|B_r(u)|=\sum_{i=0}^{r}\binom{n}{i}(q-1)^i.$$

H 4.70 (**汉明界**)若 $C\subseteq\mathcal{A}^n$是一个(n, M, d)-码，其中 $|A|=q$，$d=2t+1$，试证

$$M\leqslant\frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i}.$$

4.71 字母表$\mathcal{A}$上的一个(n, M, d)-码称为**完备码**，其中$|\mathcal{A}|=q$，若它达到汉明界：

$$M=\frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i}.$$

试证例4.113中的汉明$[2^\ell-1, 2^\ell-1-\ell]$码是完备码.

4.72 设码C可查s个错，且可纠t个错. 试证$t\leqslant s$.

*H 4.73 若$C\subseteq F^n$是一个线性码，$w\notin F^n$. 定义$r=\min_{c\in C}\delta(w, c)$. 试举一个线性码$C\subseteq F^n$和一个字$w\in F^n$的例子，使得C得可纠$t$个错，$w\in C$，且存在不同的码字$c$, $c'\in C$，满足$\delta(w, c)=r=\delta(x, c')$. 可以得出结论，对一个发送的字，选择最接近它的码字来译它可能不是定义良好的.

4.74 设C是有限域F的上的一个$[n, m]$线性码，G是C的一个生成矩阵，试证$m\times n$的矩阵A也是C的生成矩阵当且仅当对某矩阵$H\in GL(n, F)$，$A=GH$.

4.75 试证F_2上的长为$m+1$的以$x-1$为生成多项式的BCH码是奇偶性检验码.

4.76 **H** (i)在$F_2[x]$中将$x^{15}-1$写成不可约多项式的乘积.

H (ii)求一个二次不可约多项式$g(x)\in F_2[x]$，并用之去定义一个15次本原单位根$\zeta\in F_{16}$.

H (iii)求F_2上一个长为15最小矩离$d(C)\geqslant 3$的BCH码C.

H 4.77 设C是例4.131中F_8上的纠2个错的理德-索罗门码. 假设有权为2的错误向量存在，试译码字$y=(\zeta^3, \zeta, 1, \zeta^3+\zeta, 0, \zeta^3, \zeta^3)$. 431

第5章　域

多项式根的研究与域的研究密切相关. 若 $f(x)\in k[x]$，其中 k 为一个域，则很自然地考虑 k 和更大的域 E 之间的关系，其中 E 是通过将 $f(x)$ 的所有根添加入 k 而得到的域. 例如，若 $E=k$，则 $f(x)$ 是 $k[x]$ 中线性因式的乘积. 我们将看到，E 和 k 之对有伽罗瓦群 $\mathrm{Gal}(E/k)$，并且此群决定了是否存在 $f(x)$ 的一个推广了二次公式的求根公式.

→5.1　经典公式

16 世纪早期，西方世界经历了一系列变革：在 1450 年左右发明了印刷术；与亚洲、非洲的贸易空前繁荣；哥伦布发现了新大陆；马丁·路德挑战罗马教皇的权威. 改革与复兴即将开始.

那时意大利半岛不是一个国家，而是一个聚集了世界各地的富有商人的城邦的联合体. 各城邦的君主们发起的公开数学竞赛是一个年代久远的传统项目. 据记录，比萨(Pisa)的莱昂那多(Leonardo，1180—1245)，也称为斐波那契(Fibonacci)，在 1225 年给出了 $x^3+2x^2+10x-20$ 的具有较好精确度的近似根. 求一个给定的三次方程

$$X^3+bX^2+cX+d=0$$

432 的根这样的问题经常被提出[⊖]，其中 b，c，d 是实数，通常是整数.

在 16 世纪初期，现代的记号是不存在的，所以求根的技艺牵涉到的不仅仅是数学的精巧，而且要克服语言上的障碍. 用字母来标明变量是韦达(F. Viète，1540—1603)在 1591 年发明的，他用辅音来表示常量，用元音来表示变量(用字母表中开始的字母 a，b，c，…表示常量，用字母表中后面的字母 x，y，z 表示变量，这种现代记号是笛卡儿于 1637 年在他的书《La Géométrie》中引入的)，指数记号 A^2，A^3，A^4，…实际上是休谟(J. Hume)在 1636 年引入的(他表示为 A^{ii}，A^{iii}，A^{iv}，…). 符号+，－，$\sqrt{\ }$ 及诸如 a/b 中表示除法的/是魏德曼(J. Widman)在 1486 年引入的. 用符号×表示乘法是奥奇德(W. Oughtred)在 1631 年引入的. 用符号÷表示除法是拉恩(J. H. Rahn)在 1659 年引入的. 符号＝是理科德(Oxford don Robert Recorde)于 1557 年在他的书《Whetstone of Wit》中引入的：

> 为避免令人厌烦地重复"等于"一词，我经常在我的著作中用一对平行的或两条相等的线段(即＝)表示它，因为两事物相等.

这些符号并没有被立即采用，而且还有其他的类似的记号. 直到下个世纪(即 17 世纪)，当笛卡儿的书《La Géométrie》出版后，才使得大多数符号在欧洲变得通用起来.

我们回到三次方程. 缺乏好的记号确实很不方便. 例如，三次方程 $X^3+2X^2+4X-1=0$

⊖ 大约在 1074 年，奥马·海亚姆(Omar Khayyam，1048—1123)，在当今由于诗作而更有名的伊朗数学家，就用圆锥曲线给出了三次方程的根的几何构造.

只能大概地如下给出：

取某东西的 3 次方，加上此东西的平方的 2 倍，再加此东西的 4 倍，最后必须等于 1.

复杂情况更让人难以接受，负数是不允许的，方程 $X^3-2X^2-4X+1=0$ 只能用如下形式给出：$X^3+1=2X^2+4X$. 因此根据系数是正的、负的或 0(依我们的记号)，三次方程有许多形式.

以下历史来自于提格诺(J.-P. Tignol)的书《Galois' Theory of Equations》中的精彩描述：

大约在 1515 年，$X^3+mX=n$ 的代数根首先被费罗(Scipione del Ferro)获得，费罗是意大利博洛尼亚(Bologna)的数学教授，关于他本人及他的解知道甚少，因为由于某种原因，他决定不公开他的结果. 在 1526 年他死后，他的方法传给了他的一些学生. 433

此解的第二个发现通过作者本人的叙述让人们知道了更多，作者是来自布雷西亚的符塔那(Niccolò Fontana，1500—1557)，诨号"口吃者"[⊖]. 1535 年他曾经求解出了三次方程的一些特殊情形的解. 那时，他接受费罗从前的一个学生费欧(Antonio Maria Fior)的挑战，进行一个解方程的比赛，当他听说费欧已经从其老师处获得了三次方程的求解公式时，符塔那竭尽所能地求解，最后他成功地在规定时间内找出了解，给了费欧羞辱性的打击.

符塔那找到三次方程解的消息传到了卡尔达诺(Giralamo Cardano，1501—1576)耳中，卡尔达诺是一个多才多艺的科学家，他写了一系列涉及多个学科的书，包括医学、占星学、天文学、哲学及数学. 卡尔达诺要求符塔那将解给他，这样可将之收入他的一篇算术方面的论文中. 但符塔那断然地拒绝了，因为他自己打算就这个专题写一本书. 据考证，后来符塔那改变了想法，至少是部分地，因为在 1539 年，他用诗词的形式给了卡尔达诺方程 $X^3+mX=n$ 和 $xX^3=mX+n$ 的解及方程 $X^3+n=mX$ 的解的简短表示……

收到符塔那的诗后，卡尔达诺开始进一步考虑，他不仅发现了这些公式的根据，而且还解决了其他类型的三次方程的求解问题. 随后在他的划时代的专著《伟大的艺术，代数学的法则》(Ars Magna，sive de regulis algebraicis)中，他发表了他的结果，并将这个荣誉归于符塔那及费罗.

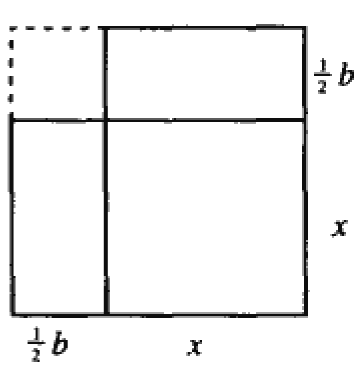


图 5-1 配方

我们先来推导低次多项式的求根公式. 推导二次求根公式的通常方法是"配方法"，且这种方法可以用文字进行叙述. 考虑二次方程 $x^2+bx+c=0$，其中 $b\geqslant 0$. 将 x^2+bx 看成图 5-1 中的面积. 通过在角上添加面积为 $\frac{1}{4}b^2$ 的小正方形就可凑成一个大正方形. 大正方形的面积为 $\left(x+\frac{1}{2}b\right)^2$. 若 $c+\frac{1}{4}b^2\geqslant 0$，则我们就构作了一个边长为 434

⊖ 原文 Tartaglia，音"塔尔塔利亚". ——译者注

$\left(x+\frac{1}{2}b\right)$面积为$c+\frac{1}{4}b^2$ 的正方形. 不用假设某些量是非负的就可以代数地完成此几何构作. 设 $f(x)=x^2+bx+c$.

$$x^2+bx+c=x^2+bx+\frac{1}{4}b^2+c-\frac{1}{4}b^2$$
$$=\left(x+\frac{1}{2}b\right)^2+\frac{1}{4}(4c-b^2).$$

因此，若 z 为 $f(x)$的一个根，则

$$z+\frac{1}{2}b=\pm\frac{1}{2}\sqrt{b^2-4c}.$$

我们现在给出二次公式的一个不同的推导方法，它是从将给定的多项式替换成一个更简单的多项式开始的.

定义 一个 n 次多项式 $f(x)\in\mathbb{R}[x]$称为是**简化的**[⊖]，若它没有 x^{n-1}项；也就是，$f(x)=a_nx^n+a_{n-2}x^{n-2}+\cdots+a_0$.

引理 5.1 作替换 $X=x-\frac{1}{n}a_{n-1}$,

$$f(X)=X^n+a_{n-1}X^{n-1}+h(X)$$

将变成一个简化的多项式

$$f^*(x)=f\left(x-\frac{1}{n}a_{n-1}\right).$$

其中 $h(X)=0$ 或 $\deg(h)\leqslant n-2$. 进一步，若 u 是 $f^*(x)$的根，则 $u-\frac{1}{n}a_{n-1}$是 $f(X)$的一个根.

证明 作替换 $X=x-\frac{1}{n}a_{n-1}$，就有

$$\begin{aligned}f^*(x)&=f\left(x-\frac{1}{n}a_{n-1}\right)\\&=\left(x-\frac{1}{n}a_{n-1}\right)^n+a_{n-1}\left(x-\frac{1}{n}a_{n-1}\right)^{n-1}+h\left(x-\frac{1}{n}a_{n-1}\right)\\&=(x^n-a_{n-1}x^{n-1}+g_1(x))+a_{n-1}(x^{n-1}+g_2(x))+h\left(x-\frac{1}{n}a_{n-1}\right)\\&=x^n+g_1(x)+a_{n-1}g_2(x)+h\left(x-\frac{1}{n}a_{n-1}\right),\end{aligned}$$

其中 $g_1(x)$，$g_2(x)$，$h\left(x-\frac{1}{n}a_{n-1}\right)$和 $g_1(x)+a_{n-2}g_2(x)+h\left(x-\frac{1}{n}a_{n-1}\right)$中的每一个或者为 0 或者是次数$\leqslant n-2$ 的多项式. 由此得出多项式 $f^*(x)=f\left(x-\frac{1}{n}a_{n-1}\right)$为简化的.

最后，若 u 为 $f^*(x)$的一个根，则 $0=f^*(u)=f\left(u-\frac{1}{n}a_{n-1}\right)$，即 $u-\frac{1}{n}a_{n-1}$为 $f(X)$的一

⊖ 若 $f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0=(x-r_1)\cdots(x-r_n)$，则 $c_{n-1}=-(r_1+\cdots+r_n)$. 因此，$f(x)$是简化的当且仅当它的根之和为 0.

个根. ■ 435

下面是二次求根公式的另一个证明.

→ **推论 5.2(二次求根公式)** *若 $f(X)=X^2+bX+c$，则它的根为*

$$\frac{1}{2}(-b\pm\sqrt{b^2-4c}).$$

证明 通过 $X=x-\frac{1}{2}b$ 定义 x，则

$$f^*(x)=\left(x-\frac{1}{2}b\right)^2+b\left(x-\frac{1}{2}b\right)+c.$$

线性项抵消了，简化的多项式为

$$f^*(x)=x^2-\frac{1}{4}(b^2-4c),$$

且 $f^*(x)$的根为 $u=\pm\frac{1}{2}\sqrt{b^2-4c}$. 引理 5.1 说 $f(X)$的根为 $u-\frac{1}{2}b$，也就是，$f(X)$的根为 $\frac{1}{2}(-b\pm\sqrt{b^2-4c})$. ■

下面这个二次求根公式的推论在推导三次求根公式时很有用.

推论 5.3 *给定数 c 和 d，则存在数 α 和 β，使得 $\alpha+\beta=c$ 及 $\alpha\beta=d$.*

证明 若 $d=0$，则取 $\alpha=0$ 和 $\beta=c$ 即可. 若 $d\neq0$，则 $\alpha\neq0$，我们可以令 $\beta=d/\alpha$，替换后即有 $c=\alpha+\beta=\alpha+d/\alpha$，从而

$$\alpha^2-c\alpha+d=0.$$

二次求根公式表明这样的 α 存在，再令 $\beta=d/\alpha$ 即可(当然，α 和 β 有可能是复数). ■

引理 5.1 简化了原来的多项式，与此同时还控制了它的根. 特别地，若 $n=3$，则 $f^*(x)$ 具有形式 x^3+qx+r.

卡尔达诺在求解简化的三次多项式的根时的“技巧”是将 x^3+qx+r 的一个根 u 写成

$$u=\alpha+\beta,$$

再去求 α 及 β. 又

$$\begin{aligned}0&=u^3+qu+r\\&=(\alpha+\beta)^3+q(\alpha+\beta)+r.\end{aligned}$$

注意

$$\begin{aligned}(\alpha+\beta)^3&=\alpha^3+3\alpha^2\beta+3\alpha\beta^2+\beta^3\\&=\alpha^3+\beta^3+3\alpha\beta(\alpha+\beta)\\&=\alpha^3+\beta^3+3\alpha\beta u.\end{aligned}$$ 436

因此，$0=\alpha^3+\beta^3+3\alpha\beta u+qu+r$，所以

$$0=\alpha^3+\beta^3+u(3\alpha\beta+q)+r. \tag{1}$$

我们已设 $\alpha+\beta=u$. 由推论 5.3，我们可以再加第二个条件，

$$\alpha\beta=-\frac{1}{3}q, \tag{2}$$

这就将方程(1)中的 u 项去掉了，剩下

$$\alpha^3+\beta^3=-r. \tag{3}$$

对方程(2)的两边取立方即有

$$\alpha^3\beta^3=-\frac{1}{27}q^3. \tag{4}$$

像在推论 5.3 中一样，带有两个未知量 α^3 和 β^3 的方程(3)及(4)可解出. 在方程(3)中作替换 $\beta^3=-q^3/(27\alpha^3)$，即有

$$\alpha^3-\frac{q^3}{27\alpha^3}=-r,$$

将其整理得

$$\alpha^6+r\alpha^3-\frac{1}{27}q^3=0, \tag{5}$$

由二次求根公式，即有

$$\alpha^3=\frac{1}{2}(-r+\sqrt{D}), \tag{6}$$

其中 $D=r^2+\frac{4}{27}q^3$. 注意 β^3 也是方程(5)中二次方程的一个根，因此

$$\beta^3=\frac{1}{2}(-r-\sqrt{D}). \tag{7}$$

取它的一个立方根[⊖]即可得到 α. 由方程(2)，$\beta=-q/(3\alpha)$，所以 $u=\alpha+\beta$.

那另外两个根呢？定理 3.49 告诉我们，若 u 为多项式 $f(x)$ 的一个根，则存在多项式 $g(x)$ 使得 $f(x)=(x-u)g(x)$. 在求出一个根 $u=\alpha+\beta$ 后，用 $x-u$ 去除 x^3+qx+r，即可得到商式 $g(x)$，再用二次求根公式求商式 $g(x)$，即可求出另外两根[$g(x)$的任意一根也是 $f(x)$的一个根.]

在这里我们给出 $f(x)$的其他两个根的一个直接公式(以替代上面刚刚给出的求解方法). 3 次单位方根有 3 个，即 1，$\omega=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$和 $\omega^2=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}$. 这样，除 α 之外 α^3 的 3 次单位方

437 根为 $\omega\alpha$ 和 $\omega^2\alpha$. 若 β 为 α 的"相伴数"，即像在(2)中一样，$\beta=-q/(3\alpha)$，则 $\omega\alpha$ 的相伴数为

$$-q/(3\omega\alpha)=\beta/\omega=\omega^2\beta,$$

$\omega^2\alpha$ 的相伴数为

$$-q/(3\omega^2\alpha)=\beta/\omega^2=\omega\beta.$$

因此 $f(x)$的根的直接公式为：$\alpha+\beta$，$\omega\alpha+\omega^2\beta$ 和 $\omega^2\alpha+\omega\beta$.

我们已经证明了三次求根公式(亦称为**卡尔达诺公式**).

→ **定理 5.4(三次求根公式)** *x^3+qx+r(其中 $q\neq 0$)的根为*

$$\alpha+\beta,\ \omega\alpha+\omega^2\beta \text{ 和 } \omega^2\alpha+\omega\beta,$$

⊖ 数 $z=\frac{1}{2}(-r+\sqrt{D})$可能是复数. 求 z 的立方根最容易的方法是将 z 写成极坐标形式 $z=s\mathrm{e}^{\mathrm{i}\theta}$，$s\geqslant 0$，则它的一个立方根为$\sqrt[3]{s}\,\mathrm{e}^{\mathrm{i}\theta/3}$.

其中 $\alpha^3=\frac{1}{2}(-r+\sqrt{D})$，$\beta=-q/(3\alpha)$，$D=r^2+\frac{4}{27}q^3$ 且 $\omega=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$ 为 3 次单位方根之一.

证明 我们已经给出了 $\alpha\neq0$ 时的证明. 由方程(2)我们有 $\alpha\beta=-q/3$，因此 $\alpha=0$ 时必有 $q=0$，也就是简化的三次式为 x^3+r，此时 $\beta^3=-r$，根为 β，$\omega\beta$ 和 $\omega^2\beta$，所以三次求根公式在此情形下也成立. ■

回忆一下，方程(7)给出 $\beta^3=\frac{1}{2}(-r-\sqrt{D})$.

二次及三次求根公式在任意系数域 k 上无效. 例如，在特征为 2 的域 k 中，因为 $2=0$，所以二次求根公式对 $k[x]$中的二次多项式无意义，因为$\frac{1}{2}$无定义. 类似地，三次求根公式(及下面的四次求根公式)不能应用于系数属于特征为 2 或 3 的域上的多项式中，因为公式含有$\frac{1}{2}$及$\frac{1}{3}$，它们在这些域中无意义.

→ **例 5.5(好的例子)** 我们来求 $x^3-15x-126$ 的根. 因为此多项式无 x^2 项，故已经是简化的，具有可以用三次求根公式的形式(若多项式不是简化的，则需要像在引理 5.1 中一样，首先将其简化). 这里$q=-15$，$r=-126$，$D=(-126)^2+4(-15)^3/27=15376$，$\sqrt{D}=124$. 因此三次求根公式给出 $\alpha^3=\frac{1}{2}[-(-126)+124]=125$ 且 $\alpha=5$. 而 $\beta=-q/3\alpha=15/(3\cdot5)=1$. 所以多项式的根为$\alpha+\beta=6$，$\omega\alpha+\omega^2\beta=-3+2\mathrm{i}\sqrt{3}$和 $\omega^2\alpha+\omega\beta=-3-2\mathrm{i}\sqrt{3}$.

也可用另一种方法求解. 在求出 $u=6$ 为一根后，应用除法算式可得

$$x^3-15x-126=(x-6)(x^2+6x+21),$$

这样二次求根公式就给出因式 $x^2+6x+21$ 的根：$-3\pm2\mathrm{i}\sqrt{3}$. ◀ 438

→ **例 5.6(差的例子)** 在例 5.5 中，用按部就班的三次求根公式方式就给出了 $x^3-15x-126$ 的根.

我们来对多项式

$$x^3-7x+6=(x-1)(x-2)(x+3)$$

用一下三次求根公式. 显然它的根为 1，2 及-3. 此多项式无 x^2 项，$q=-7$，$r=6$ 且 $D=r^2+4q^3/27=-400/27<0$. 三次求根公式给出了一个糟糕的回答：它的根是

$$\alpha+\beta,\quad \omega\alpha+\omega^2\beta \text{ 和 } \omega^2\alpha+\omega\beta,$$

其中 $\alpha^3=\frac{1}{2}\left(-6+\sqrt{\frac{-400}{27}}\right)$，且 $\beta^3=\frac{1}{2}\left(-6-\sqrt{\frac{-400}{27}}\right)$. 一些奇怪的东西出现了，存在三个奇怪的方程，它们告诉我们：1，2 及-3 中每一个数都等于上面列出的糟糕表示中的某一个. 因此

$$\omega\sqrt[3]{\frac{1}{2}\left(-6+\sqrt{\frac{-400}{27}}\right)}+\omega^2\sqrt[3]{\frac{1}{2}\left(-6-\sqrt{\frac{-400}{27}}\right)}$$

等于 1，2 或-3 中某个数. 除去 3 次复单位根不说，这个表示还牵涉到负数$-400/27$ 的平

方根.

此例子表明为什么三次公式很少使用. 尽管它的确给出了三次式的根，但它给出的形式是不可辨认的. ◀

直到中世纪，数学家们在处理二次方程时忽略负数的平方根的做法没有遇到什么困难. 例如，考虑求面积为 A 周长为 p 的长方形的边长 x 和 y 的问题. 从方程

$$xy = A \text{ 及 } 2x + 2y = p$$

可得出二次方程 $2x^2 - px + 2A = 0$. 像在推论 5.3 中一样，二次求根公式给出的根为

$$x = \frac{1}{4}(p \pm \sqrt{p^2 - 16A}).$$

若 $p^2 - 16A \geqslant 0$，人们可求出 x(及 y)；若 $p^2 - 16A < 0$，人们只是仅仅说不存在周长及面积满足这种关系的长方形. 但是三次求根公式不允许我们抛弃“虚”根，因为我们看到一个“标准”的实及正的根，甚至是正整数，可以用复数来表示⊖. 在古希腊时，毕达哥拉斯学派所说的数就
439 是正整数. 到中世纪，数可以认为是正实数(尽管对实数是什么几乎一无所知). 在数学史中三次求根公式的重要性在于它迫使数学家们严肃地考虑负数及复数.

普特南国家数学年赛的第一个获奖者、物理学家(也是诺贝尔物理奖获得者)费伊曼(R. P. Feynman, 1918—1988)建议给三次求根公式另一个可能的评价. 像在本节开始时所提及的一样，三次求根公式是在 1515 年大变革的时代被发现的. 在欧洲中世纪的黑暗时期，人们对古代希腊及罗马的文明几乎是盲目崇拜. 当时认为在很久以前人类就已取得了最高的成就，当代人比他们的祖先低能. (与现在人持有的人类不断进步的世界观正好相反!)三次求根公式实质上就是第一个古人不知道而现代人知道的数学公式，它有力地证明了 16 世纪的人与他们的祖先一样聪明.

四次求根公式是费拉理(Lodovici Ferrari, 1522—1565)在 16 世纪 40 年代早期发现的，也出现在卡尔达诺的书中，但比三次求根公式所引起的注意要少很多. 原因在于三次多项式可以解释为体积，而四次多项式没有如此明显的解释. 卡尔达诺写到：

> 正如一次方归诸于直线一样，平方归诸于平面，三次方归诸于立方体. 如果我们偏离这个观点，那将是非常愚蠢的. 大自然不允许那样. 因此……所有那些直至并且包括立方的东西是完全被证明了的. 但对于我们要加的其他的东西，我们仅仅是列示出来而已.

三次多项式 $f(x) \in \mathbb{R}[x]$的判别式是一个可发觉许多有趣的性质的数，$f(x)$的所有根是否全为实的? $f(x)$是否有重根?

定义 若 $f(x) = x^3 + qx + r = (x-u)(x-v)(x-w)$，则定义 $\Delta = (u-v)(u-w)(v-w)$，且令

$$\Delta^2 = [(u-v)(u-w)(v-w)]^2,$$

称数 Δ^2 为 $f(x)$的**判别式**.⊜

⊖ 我们在定理 1.15 中看到了类似的现象：斐波那契序列中为整数的项可以用$\sqrt{5}$表示.

⊜ 更一般地，设 $f(x) = (x-u_1)(x-u_2)\cdots(x-u_n)$ 为 n 次多项式，则 $f(x)$ 的判别式定义为 Δ^2，其中 $\Delta = \prod_{i<j}(u_i - u_j)$(取 $i<j$ 目的是使得差 $u_i - u_j$ 在乘积中出现且仅出现一次). 特别地，二次求根公式表明 $x^2 + bx + c$ 的判别式为 $b^2 - 4c$.

很自然地，我们考虑的是 Δ^2 而不是 Δ，因为 Δ 是一个不仅依赖于根而且依赖根的排序的数. 例如，如果我们将根排为 u，w，v，则 $(u-w)(u-v)(w-v)=-\Delta$，因为因子 $w-v=-(v-w)$变了符号，而平方就消去了这种差异. 440

注意当 $\Delta^2=0$ 时，$\Delta=0$，此时三次方程有重根. 我们能够不先计算根而觉察出这个性质来吗？三次求根公式使我们能够用 q 和 r 来计算 Δ^2.

引理 5.7 *$f(x)=x^3+qx+r$ 的判别式是*

$$\Delta^2=-27r^2-4q^3=-27D.$$

证明 设 $f(x)$的根为 u，v 及 w，那么由三次求根公式，

$$u=\alpha+\beta;\quad v=\omega\alpha+\omega^2\beta;\quad w=\omega^2\alpha+\omega\beta,$$

其中 $\omega=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}$，$D=r^2+\frac{4}{27}q^3$，$\alpha=\sqrt[3]{\frac{1}{2}(-r+\sqrt{D})}$且 $\beta=-\frac{1}{3}\frac{q}{\alpha}$. 易验证：

$$u-v=\alpha+\beta-\omega\alpha-\omega^2\beta=(1-\omega)(\alpha-\omega^2\beta);$$
$$u-\omega=\alpha+\beta-\omega^2\alpha-\omega\beta=-\omega^2(1-\omega)(\alpha-\omega\beta);$$
$$u-\omega=\omega\alpha+\omega^2\beta-\omega^2\alpha-\omega\beta=\omega(1-\omega)(\alpha-\beta).$$

因此

$$\Delta=-\omega^3(1-\omega)^3(\alpha-\beta)(\alpha-\omega\beta)(\alpha-\omega^2\beta).$$

当然，$-\omega^3=-1$，而

$$(1-\omega)^3=1-3\omega+3\omega^2-\omega^3=-3(\omega-\omega^2).$$

但 $\omega=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$及 $\omega^2=\overline{\omega}=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}$，所以 $\omega-\omega^2=\mathrm{i}\sqrt{3}$，因此$(1-\omega)^3=-3(\omega-\omega^2)=-3\mathrm{i}\sqrt{3}$，且

$$-\omega^3(1-\omega)^3=3\mathrm{i}\sqrt{3}.$$

最后，习题 3.85(ii)给出

$$(\alpha-\beta)(\alpha-\omega\beta)(\alpha-\omega^2\beta)=\alpha^3-\beta^3=\sqrt{D}.$$

因此 $\Delta=3\mathrm{i}\sqrt{3}\sqrt{D}$且

$$\Delta^2=-27D=-27r^2-4q^3.$$ ■

例如，我们不用三次求根公式就能看出 $f(x)=x^3-3x+2$ 有重根，因为$-27r^2-4q^3=0$. 由此也可以得出，若 $f(x)\in k[x]$，则它的判别式也在 k 中.

下面我们用判别式来判断三次多项式的根是否全为实数. 441

引理 5.8 *每一个奇次多项式 $f(x)\in\mathbb{R}[x]$至少有一个实根.*

注 *我们的证明假设了 $f(x)$有一个复根(这由代数基本定理可得).*

证明 对 $n\geqslant0$ 用归纳法，其中 $\deg(f)=2n+1$. 基础步骤 $n=0$ 时结论是显然成立的. 设 $n\geqslant1$ 且 u 为 $f(x)$的一个复根. 若 u 为实数，则已经成立，否则 $u=a+ib$，习题 5.6 表明 u 的复共轭$\overline{u}=a-ib$ 也为 $f(x)$一个根. 进一步，因为 u 不是实数，所以 $u\neq\overline{u}$. $x-u$ 和 $x-\overline{u}$都是 $f(x)$的因式，并且是互素的，所以它们的乘积也是 $f(x)$的因式，即 $f(x)$在$\mathbb{C}[x]$中有分解：

$$f(x)=(x-u)(x-\overline{u})g(x).$$

又$(x-u)(x-\bar{u})=x^2-2ax+a^2+b^2\in\mathbb{R}[x]$. 由除法算式，$g(x)=f(x)/(x-u)(x-\bar{u})\in\mathbb{R}[x]$. 因为 $\deg(g)=(2n+1)-2=2(n-1)+1$，由归纳假设 $g(x)$有一个实根，从而 $f(x)$有一个实根. ■

命题 5.9 $x^3+qx+r\in\mathbb{R}[x]$的所有根 u，v，w 均为实数当且仅当它的判别式 $\Delta^2\geqslant 0$，即 $27r^2+4q^3\leqslant 0$.

证明 如果 u，v 和 w 为实数，则 $\Delta=(u-v)(u-w)(v-w)$也是一个实数，从而 $-27r^2-4q^3=\Delta^2\geqslant 0$，即 $27r^2+4q^3\leqslant 0$.

反之，假设 $w=s+ti$ 不是实数(即 $t\neq 0$)，由下面的习题 5.6，一个根的复共轭也是根，故我们可以取 $v=s-ti$. 由引理 5.8，剩下的根 u 一定是实数. 又

$$\begin{aligned}\Delta &=(u-s+ti)(u-s-ti)[s-ti-(s+ti)]\\ &=(-2ti)[(u-s)^2+t^2].\end{aligned}$$

因为 u，s 及 t 为实数，故

$$\begin{aligned}\Delta^2 &=(-2ti)^2[(u-s)^2+t^2]^2\\ &=4t^2i^2[(u-s)^2+t^2]^2\\ &=-4t^2[(u-s)^2+t^2]^2<0,\end{aligned}$$

所以 $0>\Delta^2=-27r^2-4q^3$. 我们已经证明了若存在一个非实数的根，则 $27r^2+4q^3>0$，等价地，如果所有根为实数，则 $27r^2+4q^3\leqslant 0$. ■

下面介绍由笛卡儿给出的四次求根公式的推导.

→ **定理 5.10(四次求根公式)** *存在一个计算四次多项式*

$$X^4+bX^3+cX^2+dX+e.$$

442 *的四个根的方法.*

证明 同三次情形一样，通过令 $X=x-\frac{1}{4}b$，可将四次多项式简化为

$$x^4+qx^2+rx+s; \tag{8}$$

进一步，若 u 为第二个多项式的根，则 $u-\frac{1}{4}b$ 为第一个多项式的根.

将(8)中的 4 次多项式分解为二次多项式的积：

$$x^4+qx^2+rx+s=(x^2+jx+\ell)(x^2-jx+m) \tag{9}$$

(第二个因式中 x 的系数为 $-j$ 是因为原 4 次多项式中无 x^3 项). 若 j，ℓ 及 m 能被求出，则应用二次求根公式即可求出(8)式中四次多项式的根.

将(9)中的右边展开，由对应项系数相等能给出方程

$$\begin{cases} m+\ell-j^2 &=q;\\ j(m-\ell) &=r;\\ \ell m &=s.\end{cases} \tag{10}$$

将(10)中头两个方程相加、减，即有

$$\begin{cases} 2m=j^2+q+r/j;\\ 2\ell=j^2+q-r/j.\end{cases} \tag{11}$$

将它们代入(10)的最后一个方程：

$$\begin{aligned}4s = 4\ell m &= (j^2+q+r/j)(j^2+q-r/j)\\ &= (j^2+q)^2 - r^2/j^2\\ &= j^4+2j^2q+q^2-r^2/j^2.\end{aligned}$$

消除分母并整理，即有

$$j^6+2qj^4+(q^2-4s)j^2-r^2=0, \tag{12}$$

它是 j^2 的三次方程. 由三次求根公式可求出 j^2，应用(11)即可求出 ℓ 及 m. ■

→ **例 5.11** 考虑

$$x^4-2x^2+8x-3=0,$$

所以 $q=-2$，$r=8$ 及 $s=-3$. 若我们分解此四次多项式为：

$$(x^2+jx+\ell)(x^2-jx+m),$$ 443

则(12)给出

$$j^6-4j^4+16j^2-64=0.$$

我们可以用三次求根公式来求 j^2，但这样会很烦琐，因为我们要去掉 j^4 后才能进行其余的计算. 就这个例子而言，我们可以处理得更简洁一些. 观察到 $j=2$ 为它的一根，因为方程可写成

$$j^6-4j^4+16j^2-64=j^6-2^2j^4+2^4j^2-2^6=0$$

(许多初等教材喜欢说，在这种情况下，由"观察法"得 $j=2$). 我们现在来用(11)式求 ℓ 和 m.

$$2\ell = 4-2+(8/2)=6$$

$$2m=4-2-(8/2)=-2.$$

因此原来的四次多项式可分解为

$$(x^2-2x+3)(x^2+2x-1).$$

由二次求根公式即可给出四次多项式的根：

$$-1+\mathrm{i}\sqrt{2},-1-\mathrm{i}\sqrt{2},1+\mathrm{i}\sqrt{2} \text{ 和 } 1-\mathrm{i}\sqrt{2}.$$ ◀

不要被这个例子误导，与三次求根公式一样，找一个使其根若用四次求根公式表出是可辨认的四次多项式是很困难的. 读者可以检验，四次求根公式给出的 $x^4-25x^2+60x-36=(x-1)(x-2)(x-3)(x+6)$的根具有非常复杂的形式.

至此对我们的前辈来说，求五次多项式 $g(X)=X^5+bX^4+cX^3+dX^2+eX+f$ 的根就是一个非常诱惑的问题了. 从作替换 $X=x-\frac{1}{5}b$ 消去四次项开始. 很自然地我们希望用一些更精巧的替换外加低次多项式的求根公式能够求出 $g(X)$的根. 但是 5 次多项式阻挡了这样的尝试几乎 300 年. 我们将在下一节中继续讲述这个故事.

韦达三次公式

利用含有开方的求根公式并不是求三次方程根的最简单方法. 我们现在给出 x^3+qx+r 的根的另一个公式，它归功于韦达(Viète)，他用余弦的赋值来代替根的开方运算(总之在它们的值需要极限的意义下，它们是"无限的"，这与"有限"域的运算不同.)由推论 1.26，我

们有

444 $$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta.$$

从而三次方程

$$y^3 - \frac{3}{4}y - \frac{1}{4}\cos(3\theta) \tag{13}$$

的一个根为 $u=\cos\theta$. 由习题 5.8，此特殊的三次方程的另外两个根为 $u=\cos(\theta+120°)$ 及 $u=\cos(\theta+240°)$.

设 $f(x)=x^3+qx+r$ 为一个所有根为实数的三次多项式(命题 5.9 给出了一个判别此种情形出现的方法). 我们来将 $f(x)$ 转化为(13)的形式. 若 v 为 $f(x)$ 的一根，设

$$v = tu,$$

其中 t 和 u 待定⊖. 代入即得

$$0 = f(tu) = t^3u^3 + qtu + r,$$

所以

$$u^3 + (q/t^2)u + r/t^3 = 0;$$

也就是 u 为 $g(y)=y^3+(q/t^2)y+r/t^3$ 的一根. 若我们选择 t 使得

$$q/t^2 = -\frac{3}{4}, \tag{14}$$

且对某 θ,

$$r/t^3 = -\frac{1}{4}\cos(3\theta) \tag{15}$$

则它的根为

$$u = \cos\theta, \quad u = \cos(\theta+120°) \text{ 及 } u = \cos(\theta+240°).$$

但若 $u^3+(q/t^2)u+r/t^3=0$，则 $t^3u^3+qtu+r=0$，也就是说，$f(x)=x^3+qx+r=0$ 的根 $v=tu$ 是

$$v = tu = t\cos\theta, \quad v = t\cos(\theta+120°) \text{ 和 } v = t\cos(\theta+240°).$$

我们现在来求 t 和 u. 方程(14)给出 $t^2=-4q/3$，所以

$$t = \sqrt{-4q/3}. \tag{16}$$

由命题 5.9，$27r^2+4q^3\leqslant 0$，立即有

445 $$4q^3 \leqslant -27r^2;$$

因为右边为负的，所以 q 必定为负的. 因此 $-4q/3$ 就是正的，从而 $t=\sqrt{-4q/3}$ 为实数. (15)给出

$$\cos(3\theta) = -4r/t^3,$$

若 $|-4r/t^3|\leqslant 1$，则可确定 θ 的值. 因为 $27r^2\leqslant -4q^3$，即有 $9r^2/q^2\leqslant -4q/3$. 取平方根，因为 $t=\sqrt{-4q/3}$，所以有

$$\left|\frac{3r}{q}\right| \leqslant \sqrt{\frac{-4q}{3}} = t,$$

⊖ 费罗的技巧是将一个根写成一个和 $\alpha+\beta$，而韦达的技巧是将一个根写成一个积.

又 $t^2=-4q/3$，故

$$\left|\frac{-4r}{t^3}\right|=\left|\frac{-4r}{(-4q/3)t}\right|=\left|\frac{3r}{q}\cdot\frac{1}{t}\right|\leqslant\frac{t}{t}=1,$$

满足我们的要求. 实际上我们已经证明了下面的定理.

定理 5.12(韦达) 设 $f(x)=x^3+qx+r$ 为一个三次多项式且 $27r^2+4q^3\leqslant 0$. 若 $t=\sqrt{-4q/3}$，$\cos(3\theta)=-4r/t^3$，则 $f(x)$ 的根为：

$$t\cos\theta,\quad t\cos(\theta+120°)\text{ 和 }t\cos(\theta+240°).$$

例 5.13 再次考虑在例 4.13 中讨论过的三次方程 $x^3-7x+6=(x-1)(x-2)(x+3)$. 当然它的根为 1，2 和 -3. 求根公式给出的 3 个根的表达式相当复杂，牵涉到$\sqrt{-400/27}$这样的复数的三次方根. 让我们用定理 5.12 来求这些根(因为 $27r^2+4q^3=-400\leqslant 0$，所以可以应用定理 5.12)，我们首先计算 t 和 θ：

$$t=\sqrt{-4q/3}=\sqrt{-4(-7)/3}=\sqrt{28/3}\approx 3.055$$

且

$$\cos(3\theta)=-4r/t^3\approx -24/(3.055)^3\approx -0.842;$$

因为 $\cos(3\theta)\approx -0.842$，由三角函数表或计算器知 $3\theta\approx 148°$，从而

$$\theta\approx 49°.$$

故三次方程的根近似为

$$3.055\cos 49°,\quad 3.055\cos 169°\text{ 和 }3.055\cos 289°.$$

这些是对准确解的良好的近似. 再一次用三角函数表或计算器，我们有

$$\cos 49°\approx 0.656\text{ 且 }3.055\cos 49°\approx 2.004\approx 2.00;$$

$$\cos 169°\approx -0.982\text{ 且 }3.055\cos 169°\approx -3.00;$$

$$\cos 289°\approx 0.326\text{ 且 }3.055\cos 289°\approx 0.996\approx 1.00.$$ ◀ 446

注 由引理 5.8，每一个三次多项式 $f(x)\in\mathbb{R}[x]$有一个实根，略改韦达定理的证明就可得 $f(x)$何时有复根，也就是当判别条件是

$$-4q^3<27r^2$$

的时候.

回忆双曲函数为

$$\cosh\theta=\frac{1}{2}(e^{\theta}+e^{-\theta})$$

和

$$\sinh\theta=\frac{1}{2}(e^{\theta}-e^{-\theta}).$$

我们在前面看到，对所有 θ，$\cosh\theta\geqslant 1$，可以证明 $\sinh\theta$ 可取值为任何一个实数. 这些函数满足下面的三次方程(习题 5.9)：

$$\cosh(3\theta)=4\cosh^3(\theta)-3\cosh(\theta)$$

和

$$\sinh(3\theta)=4\sinh^3(\theta)+3\sinh(\theta).$$

由上面第一个三次方程，可见 $h(y)=y^3-\frac{3}{4}y-\frac{1}{4}\cosh(3\theta)$ 有一根为 $u=\cosh(\theta)$. 为将 $f(x)=x^3+qx+r$ 变形为 $h(y)$，我们记 $f(x)$ 的实根 v 为 $v=tu$. 与在韦达定理的证明中一样，我们有 $t^2=-4q/3$ 且 $\cosh(3\theta)=-4r/t^3$.

若 $-4q/3\geqslant 0$，则 t 为实数，应用判别条件 $-4q^3<27r^2$ 可以证明 $-4r/t^3\geqslant 1$. 因此存在数 φ 使得 $\cosh(\varphi)=-4r/t^3$，因此 $f(x)$ 的实根由下式给出

$$v=t\cosh(\varphi/3),$$

其中 $t=\sqrt{-4q/3}$. [当然，$f(x)$ 另外两个(复)根为二次多项式 $f(x)/(x-v)$ 的根.]

若 $-4q/3<0$，则我们用双曲正弦函数. 我们知道 $\sinh(\theta)$ 是 $k(y)=y^3+\frac{3}{4}y-\frac{1}{4}\sinh(3\theta)$ 的一根. 为将 $f(x)$ 变形为 $k(y)$，我们记 $f(x)$ 的实根 v 为 $v=tu$，其中 $t=\sqrt{4q/3}$(我们现在的假设可推出 $4q/3>0$)且 $\sinh(3\theta)=-4r/t^3$. 同我们前面注解的一样，存在一个数 γ 使得 $\sinh(\gamma)=-4r/t^3$，所以此时 $f(x)$ 的实根为

447 $$v=t\sinh(\gamma/3).$$ ◀

习题

5.1 (i)求 $f(x)=x^3-3x+1$ 的根.

H (ii)求 $f(x)=x^3-9x+28$ 的根. 答案：-4，$2\pm i\sqrt{3}$.

(iii)求 $f(x)=x^3-24x^2-24x-25$ 的根. 答案：17，$-\frac{1}{2}\pm i\frac{\sqrt{3}}{2}$.

5.2 (i)用三次公式求 $f(x)=x^3-15x-4$ 的根. 答案：$g=\sqrt[3]{2+\sqrt{-121}}$ 和 $h=\sqrt[3]{2-\sqrt{-121}}$.

(ii)用三角公式求 $f(x)$ 的根. 答案：4，$-2\pm\sqrt{3}$.

5.3 求 $f(x)=x^3-6x+4$ 的根. 答案：2，$-1\pm\sqrt{3}$.

5.4 求 $x^4-15x^2-20x-6$ 的根. 答案：-3，-1，$2\pm\sqrt{6}$.

*5.5 下面的城堡问题出现于一本旧的中国教材中，它是由数学家秦九韶在 1247 年解决的. 有一个圆形的城堡，其直径未知. 城堡有 4 个门，在北大门的 2 单位长外有一棵大树，从距南大门 6 单位长的东边可看到此大树. 问此城堡的直径是多少?

(i)试证城堡的半径 r 是三次多项式 X^3+X^2-36 的一个根.

(ii)试证 $f(X)=X^3+X^2-36$ 有一个根是整数，并求另外两个根. 将你的方法与用卡尔达诺公式和韦达的三角法的解答作比较.

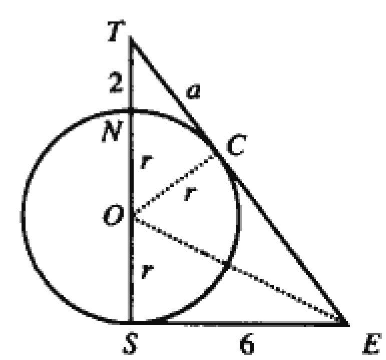


图 5-2 城堡问题

*H 5.6 试证若 u 为多项式 $f(x)\in\mathbb{R}[x]$ 的一根，则其复共轭 $\bar{u}$ 也是 $f(x)$ 的一根.

*5.7 设 $0\leqslant 3\alpha<360°$.

(i)若 $\cos 3\alpha$ 为正的，证明存在一个锐角 β，使得 $3\alpha=3\beta$ 或 $3\alpha=3(\beta+90°)$ 并且数集

$$\cos\beta,\quad \cos(\beta+120°),\quad \cos(\beta+240°)$$

与数集

$$\cos(\beta+90°),\quad \cos(\beta+210°),\quad \cos(\beta+330°)$$

448 相同.

(ii)若 $\cos 3\alpha$ 为负的，证明存在一个锐角 β，使得 $3\alpha=3(\beta+30°)$ 或 $3\alpha=3(\beta+60°)$ 并且数集

$$\cos(\beta+30°),\quad \cos(\beta+150°),\quad \cos(\beta+270°)$$

与数集

$$\cos(\beta+60°),\quad \cos(\beta+180°),\quad \cos(\beta+270°)$$

相同.

*H 5.8 试证：若 $\cos3\theta=r$，则 $4x^3-3x-r$ 的根为

$$\cos\theta,\quad \cos(\theta+120°) \text{ 和 } \cos(\theta+240°).$$

*5.9 H (i)证明 $\cosh(3\theta)=4\cosh^3(\theta)-3\cosh(\theta)$.

H (ii)证明 $\sinh(3\theta)=4\sinh^3(\theta)+3\sinh(\theta)$.

H5.10 求 $x^3-9x+28$ 的根.

H5.11 求 $x^3-24x^2-24x-25$ 的根.

5.12 H (i)用三次求根公式求 $x^3-15x-4$ 的根.

H (ii)用三角公式求上面多项式的根.

H5.13 求 x^3-6x+4 的根.

H5.14 求 $x^4-15x^2-20x-6$ 的根.

→5.2 一般五次方程的不可解性

从 16 世纪初期到 19 世纪初期，数学家们花了几乎 300 年的时间来寻找二次、三次及四次求根公式的推广，以便求解出任何多项式的根. 最终，鲁费尼(P. Ruffini，1765—1822)在 1799 年和阿贝尔(N. H. Abel，1802—1829)在 1824 年都证明了对一般的五次方程不存在这样的公式(尽管他们的证明都有漏洞，但阿贝尔的证明被他同时代的人接受了，而鲁费尼的没有). 伽罗瓦(E. Galois，1811—1832)在去世之前有能力准确地确定那些多项式，它们的根可以由牵涉数的平方根、立方根、四次根……及普通数域的加、减、乘、除的运算的公式求出. 为达到此目的，他也创立了群论.

若 $f(x)\in k[x]$是一个首一多项式，其中 k 是一个包含 $f(x)$的所有根 z_1，z_2，…，z_n(可能有重复)的域，则

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=(x-z_1)\cdots(x-z_n).$$

对 $n\geqslant1$ 用归纳法，我们很容易将习题 3.102 推广为： [449]

$$\begin{aligned}
a_{n-1}&=-\sum_i z_i\\
a_{n-2}&=\sum_{i<j}z_iz_j\\
a_{n-3}&=-\sum_{i<j<k}z_iz_jz_k\\
&\ \ \vdots\\
a_0&=(-1)^n z_1z_2\cdots z_n.
\end{aligned}\tag{1}$$

注意 $-a_{n-1}$是所有根的和，$\pm a_0$ 是所有根的积. 给定 $f(x)$的系数，能否求出 $f(x)$的根？即给定 a，能否解出带有 n 个未知数的 n 个方程组成的方程组(1)？若 $n=2$，且 k 的特征不是 2，回答是“可以”：可用二次求根公式(这就是推论 5.3). 若 $n=3$ 或 4，且 k 的特征不是 2 或 3，则回答也是“可以”，因为可用三次和四次求根公式. 但若 $n\geqslant5$，我们将看到没有类似的解

存在.

我们不是说当 $n \geqslant 5$ 时，方程组(1)无解，而是说不存在能用类似于经典公式表示的解. 我们已经看到：若我们限制自己用一种特殊的方式使用特殊的工具，经典的古希腊问题是不可能解决的. 但若我们放松限制(如我们已经看到阿基米德是如何三等分角的)，这些问题是可解决的. 类似地，若我们不限制只用域中的运算及根的开方，那么存在一个求解一个多项式的根的方法是相当有可能的. 例如，我们已经看到，三次多项式的韦达三角解. 事实上，我们可用牛顿法来求任意一个多项式 $f(x) \in \mathbb{R}[x]$ 的实根：若 r 为 $f(x)$ 的一个实根且 h_0 是 r 的一个"好"的近似值，则 $r = \lim_{n \to \infty} h_n$，其中规定 $h_{n+1} = h_n - f(h_n)/f'(h_n)$. 有利用椭圆模函数求 5 次方程根的埃尔米特法，也有使用超几何函数来求多个更高次多项式的根的方法. 一旦我们给出了准确的定义，我们马上证明，若 $n \geqslant 5$，则"用根式"求解并不总是可行的.

让我们回忆前几章中的几个定义和命题. 若 k 为域 K 的一个子域，则我们通常说 K 为 k 的一个**扩张**，我们简记为"K/k 是一个扩张". 若 K/k 是一个扩张，则与例 4.1(iii)中一样，K 可以看成 k 上的一个向量空间. 称 K 为 k 的一个**有限扩张**若 K 是 k 上的一个有限维向量空间，
450 K 的维数，记为 $[K:k]$，称为 K/k 的**次数**.

→ **例 5.14** 设 $p(x) \in k[x]$ 为一个 n 次不可约多项式，k 为一个域，且设 $k(z)/k$ 为添加 $p(x)$ 的一个根 z 的一个扩张. 命题 3.116(iv)说 $k(z)$ 中的每个元素有唯一的表示 $b_0 + b_1 z + \cdots + b_{n-1} z^{n-1}$，其中 $b_i \in k$. 因此，表 $1, z, z^2, \cdots, z^{n-1}$ 是 $k(z)/k$ 的一组基，故 $\dim(k(z)) = n = \deg(p)$. ◀

为方便读者，我们给出几个我们要用的来自第 4 章的结论.

定理 4.31 *设 $k \subseteq K \subseteq E$ 为域，K 为 k 上的有限扩张，E 是 K 上的有限扩张. 则 E 为 k 上的有限扩张，且*

$$[E:k] = [E:K][K:k].$$

定义 *设 K/k 为一个扩张且 $z \in K$. 我们称 z 为 k 上的***代数元***，若存在以 z 为根的非零多项式 $f(x) \in k[x]$，否则称 z 为 k 上的***超越元***.*

在第 3 章中，我们考虑了添加一个元素至一个域中，较详细地研究了 $k(z)$. 下面我们来推广此结论，添加一个集合的元素至一个域中. 当我们将给定的多项式的根的集合添加至一个域中时，这显得特别有意义.

→ **定义** *设 k 为域 K 的子域，$\{z_1, \cdots, z_n\}$ 为 K 的一个子集.* **添加** *$z_1, \cdots, z_n$ 到 k 而得到的 K 的子域，记为 $k(z_1, \cdots, z_n)$，是 K 的所有包含 k 及 $z_1, \cdots, z_n$ 的子域的交.*

当然，$k(z_1, \cdots, z_n)$ 是 K 的包含 k 及所有 z_i 的最小的子域，也就是说，若 K 的子域 S 包含 k 及这些 z_i，则 $k(z_1, \cdots, z_n) \subseteq S$.

命题 4.32 *若 K/k 是一个有限扩张，则每一个 $z \in K$ 是 k 上的代数元. 反之，若 $K = k(z_1, \cdots, z_n)$ 且每一个 z_i 是 k 上的代数元，则 K/k 是一个有限扩张.*

由克罗内克定理，对给定的 $f(x) \in k[x]$，其中 k 是一个域，存在一个包含 $f(x)$ 的所有根的扩张 K/k. 也就是说，多项式 $f(x)$ 是 $K[x]$ 中线性因式的乘积.

→ **定义** *设 k 为域 K 的一个子域，且设 $f(x) \in k[x]$. 我们称 $f(x)$* **在 K 中分裂**，*如果*

$$f(x)=a(x-z_1)\cdots(x-z_n),$$

其中 z_1，…，z_n 在 K 中且 $a\in k$.

扩张 E/k 称为 **$f(x)$在 k 上的一个分裂域**，若 $f(x)$在 E 上分裂，但是在 E 的任何真子域上不分裂. 451

→ **例 5.15** 设 $m\geqslant 1$，k 为一个域，且 $f(x)=x^m-1\in k[x]$. 由克罗内克定理，存在扩张 K/k 使得$f(x)$在其上分裂. 当然 $f(x)$的根为 m 次单位根. 回忆定理 3.55 说，K 包含了一个 m 次本原单位根；也就是存在某个 m 次单位根，不妨设 $z\in K$，使得每一个 m 次单位根都是 z 的一个方幂. 换言之，所有 m 次单位根形成一个乘法循环群，一个 m 次本原单位根就是一个生成元.

设 p 是一个素数，考虑 $g(x)=x^p-1$. 若 k 的特征$\neq p$，则 $g(x)$无重根[由习题 3.67，$g(x)$无重根当且仅当$(g, g')=1$，其中 $g'(x)$是 $g(x)$的导数]. 另一方面，若 k 的特征$=p$，则 $x^p-1=(x-1)^p$，因此 $g(x)$有唯一的 p 次单位根，也就是 1.

现在考虑 $h(x)=x^p-a\in k[x]$. 设 $k(u)$是添加 u 至 k 而得到的扩张，其中 $u^p=a$. 若 k 的特征$\neq p$ 且 k 包含 p 次单位根，则我们断言 $k(u)$是 $h(x)$在 k 上的一个分裂域. 若 z 是一个本原单位根，则 $h(x)$的根为 u，zu，z^2u，…，$z^{p-1}u$. 因此，$k(u)$是 $h(x)$在 k 上的一个分裂域. 另一方面，若 k 的特征$=p$，则 $h(x)=x^p-a=x^p-u^p=(x-u)^p$，所以 $h(x)$存在唯一的根，从而在这种情况下 $k(u)$也是 $h(x)$在 k 上的一个分裂域. ◀

→ **命题 5.16** *若 $f(x)\in k[x]$，其中 k 是一个域，则 $f(x)$的分裂域 E/k 存在.*

证明 由克罗内克定理，即定理 3.118，存在一个扩张 K/k 使得在 $K[x]$中，$f(x)=a(x-z_1)\cdots(x-z_n)$. 若我们定义 $E=k(z_1, \cdots, z_n)$，其中 z_1，…，z_n 为 $f(x)$的根，则 $f(x)$在 E 上分裂. 若 $B\subsetneq E$ 是 E 的真子域，则有某 $z_i\notin B$，故 $f(x)$在 B 上不能分裂，因此，E 是 $f(x)$的一个分裂域. ■

因此 $f(x)\in k[x]$的分裂域就是 K 的包含 k 及 $f(x)$的所有根的最小子域 E. 例如，考虑 $f(x)=x^2+1\in\mathbb{Q}[x]$. $f(x)$的根为$\pm$i，因此 $f(x)$在$\mathbb{C}$上分裂，即 $f(x)=(x-\mathrm{i})(x+\mathrm{i})$为$\mathbb{C}[x]$上的线性多项式的乘积. 然而$\mathbb{C}$不是 $f(x)$的分裂域，因为$\mathbb{C}$并不是包含$\mathbb{Q}$及 $f(x)$的所有根的最小域，$\mathbb{Q}(\mathrm{i})$才是 $f(x)$的一个分裂域.

我们在分裂域的定义中说的是“一个”分裂域，而不说“这个”分裂域，其原因就是分裂域的定义不仅牵涉到 $f(x)$及 k，而且牵涉到更大的域 K. 若 $f(x)$在 $K[x]$中分裂，其中 K/k 为一个域扩张，则命题 5.16 的证明表明，包含在 K 中的分裂域存在且唯一，即 $E=k(z_1, \cdots, z_n)$. 然而，若不给定这样的 K，则分裂域可能不同. 事实上，我们在定理 5.23 中将看到，$f(x)$在 k 上的任两个分裂域都是同构的. 用这样的技术处理使我们能够证明任何两个元素个数相等的有限域是同构的. 452

→ **例 5.17** 设 $E=F(y_1, \cdots, y_n)$为系数在 F 中的关于 n 个变量 y_1，…，y_n 的所有有理函数构成的域，即 $E=\mathrm{Frac}(F[y_1, \cdots, y_n])$，它是 n 个变量的多项式环的分式域. $f(x)=(x-y_1)(x-y_2)\cdots(x-y_n)$的系数记为 a_i，由(1)可知这些 a_i 可用所有的 y_i 来给出. 定义 $k=F(a_0, \cdots, a_{n-1})$. 注意 E 是 $f(x)$在 k 上的一个分裂域，因为它是将 $f(x)$的所有根，即所有 y_i，添入 k 而得的. ◀

→ **定义** 设 E 是包含子域 k 的一个域，E 的一个**自同构**[⊖]是指同构映射 $\sigma: E\to E$. 称 σ **固定** k，若对每一个 $a\in k$，$\sigma(a)=a$.

→ **注** 若 E/k 是一个域扩张，例 4.1(iii)表明，E 是 k 上的一个向量空间. 若 $\sigma: E\to E$ 是固定 k 的一个自同构，则 σ 是一个线性变换. 显然，对所有的 z，$z'\in E$，$\sigma(z+z')=\sigma(z)+\sigma(z')$. 但是 σ 也保持纯量乘积：若 $a\in k$，则

$$\sigma(az)=\sigma(a)\sigma(z)=a\sigma(z),$$

因为 σ 固定 k.

我们已经看到，$x^2+1\in\mathbb{Q}[x]$的分裂域是 $E=\mathbb{Q}(i)$. 复共轭 $\sigma: a\mapsto\bar{a}$就是 E 的固定$\mathbb{Q}$的一个自同构.

→ **命题 5.18** 设 k 为域 K 的一个子域. 设

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in k[x],$$

又设 $E=k(z_1, \cdots, z_n)$为 $f(x)$的一个分裂域. 若 $\sigma: E\to E$ 为固定 k 的一个自同构，则 σ 置换 $f(x)$的根 $z_1, \cdots, z_n$.

证明 若 z 为 $f(x)$的一个根，则

$$0=f(z)=z^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0.$$

用 σ 作用此方程，因为 σ 固定 k，故有

$$\begin{aligned}0&=\sigma(z)^n+\sigma(a_{n-1})\sigma(z)^{n-1}+\cdots+\sigma(a_1)\sigma(z)+\sigma(a_0)\\&=\sigma(z)^n+a_{n-1}\sigma(z)^{n-1}+\cdots+a_1\sigma(z)+a_0,\end{aligned}$$

因此 $\sigma(z)$是 $f(x)$的一个根. 若 Z 是所有根的集合，则 $\sigma': Z\to Z$，其中 σ'是 σ 对 Z 的限制$\sigma|Z$.
453 但是 σ'是单射(因为 σ 是单射)，所以由习题 2.13 知道，σ'是一个置换. ■

→ **推论 5.19** 设 $k\subseteq B\subseteq F$ 为一个域塔，其中 B 是某多项式 $f(x)\in k[x]$的一个分裂域. 若 $\sigma: F\to F$ 是固定 k 的一个自同构，则 $\sigma(B)=B$.

证明 注意由命题 5.18 知 $\sigma(B)\subseteq B$，因为 σ 置换 $f(x)$的根 $z_1, \cdots, z_n$. 作为 k 上的向量空间，我们有 $B\cong\sigma(B)$，因为 σ 是一个单的线性变换. 由于$[B:k]<\infty$，由习题 5.24 可知 B 和$\sigma(B)$都是有限维的，且 $\dim(B)=\dim(\sigma(B))$. 由推论 4.25(iii)即有 $B=\sigma(B)$. ■

下面这个命题以后有用.

→ **命题 5.20** 设 $E=k(z_1, \cdots, z_n)$. 若 $\sigma: E\to E$ 是一个固定 k 的自同构且对所有 i 有 $\sigma(z_i)=z_i$，则 σ 为恒等变换.

证明 对 $n\geq 1$ 用归纳法. 若 $n=1$，则每个 $u\in E$ 具有形式 $f(z_1)/g(z_1)$，其中 $f(x)$，$g(x)\in k[x]$且 $g(z_1)\neq 0$. 但 σ 固定 z_1，也固定 $f(x)$，$g(x)$的系数，所以 σ 固定所有的 $u\in E$. 下面证明归纳步骤，记 $K=k(z_1, \cdots, z_{n-1})$. 注意 $E=K(z_n)$[因为 $K(z_n)$是包含 k 及 $z_1, \cdots, z_{n-1}$，z_n 的最小的子域]. 将 K 代替 k，重复 $n=1$ 情形的证明，即得证. ■

→ **定义** 设 k 为域 E 的一个子域. E 在 k 上的**伽罗瓦群**，记为 $\mathrm{Gal}(E/k)$，就是所有 E 的固定 k 的自同构组成的集合. 若 $f(x)\in k[x]$，$E=k(z_1, \cdots, z_n)$为它的一个分裂域，则 $f(x)$在

⊖ 原文为"automorphism". 单词"automorphism"由两个希腊字根组成，"auto"意为"自己(self)"，"morph"意为"形状(shape)"或"形式(form)". 就像一个同构将一个群映到一个完全相同的群一样，一个自同构将一个群映到自身.

k 上的伽罗瓦群就规定为 Gal(E/k).

易证 Gal(E/k)关于变换的合成构成一个群. 这个定义归于阿廷(E. Artin, 1898－1962), 与他和诺特(E. Noether)强调"抽象"的代数是一致的. 伽罗瓦原来的定义(与之同构的一个群)是用多项式的根的某些置换来叙述的, 而不是用自同构(见提格诺尔(Tignol)的《代数方程的伽罗瓦理论》(Galois' Theory of Algebraic Equations)的第 235 页－254 页)来叙述的.

例如, 若 $f(x)=x^2+1\in\mathbb{Q}[x]$, 则复共轭 σ 就是它的分裂域 $\mathbb{Q}(i)$ 的一个自同构, σ 固定 $\mathbb{Q}$ (互换根 i, －i). 因为 Gal($\mathbb{Q}(i)/\mathbb{Q}$)是对称群 S_2 的一个子群, 且阶为 2, 所以 Gal($\mathbb{Q}(i)/\mathbb{Q}$) $=\langle\sigma\rangle\cong\mathbb{I}_2$. 我们应该将 Gal($E/k$)的元素看成复共轭的推广.

定理 5.21 若 $f(x)\in k[x]$的次数为 n, 则它的伽罗瓦群 Gal(E/k)同构于 S_n 的一个群. 454

证明 设 E/k 为 $f(x)$在 k 上的一个分裂域, 设 $X=\{z_1, \cdots, z_n\}$为 $f(x)$在 E 上的不同根的集合. 若 $\sigma\in$ Gal(E/k), 那么由命题 5.18, 它在 X 上的限制 $\sigma|X$ 是 X 的一个置换, 即 $\sigma|X\in S_X$. 定义 φ: Gal(E/k)$\to S_X$ 为 $\varphi:\sigma\mapsto\sigma|X$. 为了证明 φ 为一个同态, 注意 $\varphi(\sigma\tau)$和 $\varphi(\sigma)\varphi(\tau)$均为 $X\to X$ 的函数, 所以若它们在每一个 $z_i\in X$ 上的作用一致, 则它们就是相等的. 由于 $\varphi(\sigma\tau): z_i\mapsto(\sigma\tau)(z_i)$, 而 $\varphi(\sigma)\varphi(\tau): z_i\mapsto\sigma(\tau(z_i))$, 所以它们是相同的.

φ 的像就是 $S_X\cong S_m$ 的一个子群, 其中 $m=|X|\leqslant n$[若 $f(x)$有重根, 则 $m<n$]. φ 的核就是由所有在 X 上是恒等置换的 $\sigma\in$ Gal(E/k)的组成, 即 σ 固定每一个根 z_i. 又由伽罗瓦群的定义, σ 也固定 k. 再由命题 5.20, 就有 $\ker\varphi=\{1\}$, 因此 φ 为一个单射, 也就是 Gal(E/k)同构于 S_m 的一个子群. 若 $m=n$, 则证明完成. 若 $m<n$, 也就是 $f(x)$有重根, 应用 S_m 是 S_n 的一个子群的事实. 例如, S_m 同构于 S_n 中由固定 $m+1, \cdots, n$ 的所有置换构成的子群. 因此当 $f(x)$有重根时, 定理也成立. 从而定理得证. ■

我们现在来比较一个多项式在一个给定的域 k 上的不同的分裂域. $f(x)\in k[x]$的分裂域 E 的定义是用域的扩张 K/k 来定义的, $f(x)$在 $K[x]$中可分解为线性因式的积. 若在开始时 K 没有被给定, 那么分裂域是什么? 例如, 假设 $k=\mathbb{C}(x)$, $f(y)=y^2-x$ 或 $k=\mathbb{F}_3$, $f(x)=x^9-x\in\mathbb{F}_3[x]$. 克罗内克定理(即定理 3.118)给出 $\mathbb{C}(x)$的一个包含 $\sqrt{x}$ 的域扩张, 且它还给出了 $\mathbb{F}_3$ 的一个包含 $f(x)=x^9-x$ 的所有根的域扩张. 这些域扩张没有一个是唯一的. 例如, 在例 3.121 中, 我们给出了 $f(x)$在 $\mathbb{F}_3$ 上的几个分裂域. 然而我们马上来证明, 在同构意义下, 分裂域是不依赖于扩域 K 的选择的.

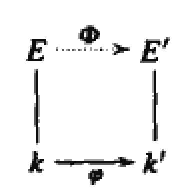
下一个结论是构造 Gal(E/k)中的自同构, 并且计算当 k 的特征为 0 时它们的数量.

回忆定理 3.33: 若 R, S 为交换环, $\varphi: R\to S$ 为一个同态, 则

$$\varphi^*: f(x)=r_0+r_1x+r_2x^2+\cdots$$
$$\mapsto\varphi(r_0)+\varphi(r_1)x+\varphi(r_2)x^2+\cdots=f^*(x),$$

是 $\varphi^*: R[x]\to S[x]$的一个同态. 若 φ 为一个同构, 则 φ^* 也是.

命题 5.22 设 $f(x)\in k[x]$, E 为 $f(x)$在 k 上的一个分裂域. 设 $\varphi: k\to k'$为一个域同构, $\varphi^*: k[x]\to k'[x]$为由定理 3.33 给出的同构 $g(x)\mapsto g^*(x)$且 E'为 $f^*(x)$在 k'的分裂域. 455



(i)存在一个扩展 φ 的同构 $\Phi: E\to E'$.

(ii)若 k 的特征为 0，则恰好存在$[E:k]$个扩张了 φ 的同构 $\Phi: E\to E'$.

证明 (i)对$[E:k]$用归纳法. 若$[E:k]=1$，则 $f(x)$是 $k[x]$中线性多项式的乘积，从而易见 $f^*(x)$也是 $k'[x]$中线性多项式的乘积，因此我们可设 $\Phi=\varphi$.

对于归纳步，取 $f(x)$在 E 中但不在 k 中的一个根 z. 设 $p(x)$是 $k[x]$中以 z 为一根的不可约多项式(命题 3.116(i)). 因为 $z\notin k$，所以 $\deg(p)>1$. 进一步，由例 5.14，$[k(z):k]=\deg(p)$. 设 $p^*(x)$为 $k'[x]$中相应的不可约多项式，z'为 $p^*(x)$在 E'中的一个根. 因为同构 $\varphi^*: k[x]\to k'[x]$将不可约多项式映为不可约多项式，因此 $p^*(x)$是不可约的.

由习题 3.101，则存在扩展了 φ 的同构 $\tilde{\varphi}: k(z)\to k'(z')$满足 $\tilde{\varphi}(z)=z'$. 现在我们将 $f(x)$看成 $k(z)$上面的多项式(因为 $k\subseteq k(z)$推出 $k[x]\subseteq k(z)[x]$). 我们断言 E 就是 $f(x)$在 $k(z)$上的分裂域，即

$$E=k(z)(z_1,\cdots,z_n),$$

其中 z_1, …, z_n 为 $f(x)$的根. 显然，

$$E=k(z_1,\cdots,z_n)\subseteq k(z)(z_1,\cdots,z_n).$$

下面证明反包含. 因为 $z\in E$，所以

$$k(z)(z_1,\cdots,z_n)\subseteq k(z_1,\cdots,z_n)=E.$$

但由定理 4.31 知$[E:k(z)]<[E:k]$，所以由归纳假设，存在同构 $\Phi: E\to E'$，它是 $\tilde{\varphi}$ 的扩展，从而也为 φ 的扩展.

(ii)此部分的证明是再次对$[E:k]$用归纳法. 若$[E:k]=1$，则 $E=k$，仅存在一个扩张，即 $\Phi=\varphi$. 若$[E:k]>1$，设在 $k[x]$中 $f(x)=p(x)g(x)$，其中 $p(x)$具有最高次数，设其为 d 的不可约因式. 我们可以假设 $d>1$，否则 $f(x)$在 k 上已经分裂了且$[E:k]=1$. 选择$p(x)$的一个根 $z\in E$(这是可能的，因为 E/k 是 $f(x)=p(x)g(x)$的一个分裂域). 与(i)中一样，多项式 $p^*(x)\in k'[x]$是不可约的且 $p^*(x)$有某根 z'在 E'中. 因为 k 的特征为 0，习题 3.95 表明，
456 $p(x)$和 $p^*(x)$无重根，也就是，每一个都有 d 个不同的根. 由命题 3.116(iii)，存在扩展了 φ 的 d 个自同构 $\tilde{\varphi}: k(z)\to k'(z')$，每一个根对应一个，而无其他的扩展了 φ 的自同构存在，因为这样的扩展一定将 z 映到某个 z'上，此时命题 5.20 证明了，它就是这些 $\tilde{\varphi}$ 中的一个. 与(i)中一样，E 就是 $f(x)$在 $k(z)$上的分裂域，E'可看成 $f^*(x)$在 $k'(z')$上的分裂域. 但是$[E:k]=[E:k(z)][k(z):k]=[E:k(z)]d$，所以$[E:k(z)]<[E:k]$. 由归纳假设，每一个 $\tilde{\varphi}$ 恰好有$[E:k(z)]$个扩张. 因此我们获得了$[E:k(z)][k(z):k]=[E:k]$个这样的扩张 Φ. 若 $\tau: E\to E'$是 φ 的另一个扩张，则对 $p^*(x)$的某个根 z'有 $\tau(z)=z'$. 因此 τ 是满足 $\tilde{\varphi}(z)=z'$ 的某个 $\tilde{\varphi}$，而这样的扩张 $E\to E'$已经计算过了. ■

在证明命题 5.22(ii)中，k 的特征为 0 的假设保证了 $k[x]$中的不可约多项式无重根. 比此更弱的陈述称为可分性，它给出了一个更好的定理. 例如，每一个有限域 k 满足此假设[见习题 5.31(iii)].

→ **定理 5.23** 若 k 为一个域，$f(x)\in k[x]$，则 $f(x)$在 k 上的任意两个分裂域是同构的.

证明 设 E, E'为 $f(x)$在 k 上的分裂域. 取 φ 为恒等变换，应用定理 5.22(i)立即可得. ■

推论 5.24 多项式 $f(x)\in k[x]$的伽罗瓦群 Gal(E/k)只依赖于 $f(x)$及 k，而不依赖于 E

的选择.

证明 若 $\varphi: E\to E'$ 为一个固定 k 的同构，则存在 $\mathrm{Gal}(E/k)\to\mathrm{Gal}(E'/k)$ 的同构：$\sigma\mapsto\varphi\sigma\varphi^{-1}$. ■

值得指出的是下一个定理直至十九世纪九十年代才被证明，距伽罗瓦发现有限域已有 60 年之久了.

→ **推论 5.25(穆尔)** 任何两个元素个数恰好为 p^n 的有限域是同构的.

证明 设 E 是一个有 $q=p^n$ 个元素的域，对乘法群 $E^\times$ 应用拉格朗日定理可得，对每一个 $a\in E^\times$ 有 $a^{q-1}=1$. 从而 E 中每个元素都是 $f(x)=x^q-x=x(x^{q-1}-1)\in\mathbb{F}_p[x]$的根，所以 E 是 $f(x)$在$\mathbb{F}_p$ 上的分裂域. ■

由此得出，若 $g(x)$，$h(x)\in\mathbb{F}_p[x]$是次数为 n 的不可约多项式，则$\mathbb{F}_p[x]/(g(x))\cong\mathbb{F}_p[x]/(h(x))$，因为两个域的元素个数都为 p^n.

穆尔(E. H. Moore，1862—1932)是作为一个代数学家开始他的数学生涯的，他在数学的其他许多分支也做出了重要工作，如穆尔-史密斯(Moore-Smith)收敛就是以他的部分名字命名的. 457

我们现在来计当 k 的特征为 0 时的伽罗瓦群 $\mathrm{Gal}(E/k)$的阶.

→ **定理 5.26** 设 E/k 是 $k[x]$ 中某多项式的分裂域，其中 k 是一个特征为 0 的域，则 $|\mathrm{Gal}(E/k)|=[E:k]$.

证明 这是命题 5.22(ii)在 $k=k'$，$E=E'$和 $\varphi=1_k$ 时的一个特殊情形. ■

注 当 k 的特征为 $p>0$ 时，定理 5.26 可能不成立. 当 k 是有限域时，它是成立的，但当 $k=\mathbb{F}_p(x)$，$\mathbb{F}_p$ 上的全体有理函数时它不成立. 习题 5.32 描述了一个反例. 像我们在命题 5.22 的证明之后所提及的一样，研究此问题的方法涉及可分性这一概念.

→ **推论 5.27** 设 $f(x)\in k[x]$是一个次数为 n 的不可约多项式，其中 k 是特征为 0 的域. 若 E/k 是 $f(x)$在 k 上的一个分裂域，则 n 是 $|\mathrm{Gal}(E/k)|$ 的因数.

证明 若 $z\in E$ 是 $f(x)$的一个根，则像在例 5.14 中一样，$|k(z):k|=n$. 但$[E:k]=[E:k(z)][k(z):k]$，所以 $n\mid[E:k]$. 因为 k 的特征为 0，所以由定理 5.26，$|\mathrm{Gal}(E/k)|=[E:k]$. ■

若 k 一个域，则当底域 k 增大时，$k[x]$中的多项式的不可约多项式分解会变化.

引理 5.28 设 B/k 是某多项式 $g(x)\in k[x]$的一个分裂域. 若 $p(x)\in k[x]$是不可约的，且若

$$p(x)=q_1(x)\cdots q_t(x)$$

是 $p(x)$在 $B[x]$中的不可约多项式分解，则所有 $q_i(x)$的次数相同.

证明 将 $p(x)$看成 $B[x]$中的一个多项式(因为 $k\subseteq B$ 可推出 $k[x]\subseteq B[x]$)，且设 $E=B(z_1,\cdots,z_n)$为 $p(x)$的一个分裂域，其中 $z_1,\cdots,z_n$ 为 $p(x)$的根. 若 $p(x)$在 $B[x]$中不能分解，则证毕. 否则取 $q_1(x)$的一个根 z_1，对每一个 $j\neq1$，取 $q_j(x)$的一个根 z_j. 因为 z_1 和 z_j 都是不可约多项式 $p(x)$的根，所以由命题 3.116(iii)，有同构 $\varphi_j: k(z_1)\to k(z_j)$使得 $\varphi_j(z_1)=z_j$，且 φ_j 固定 k 中每一个元. 命题 5.22(i)说，φ_j 可以扩张成E 的一个自同构 Φ_j 且由推论 5.19 可知 $\Phi_j(B)=B$. 因此 Φ_j 诱导出一个同构 $\Phi_j^*: B[x]\to B[x]$(通过让 Φ_j 作用在多项式的系数上).

立即得出

458
$$p^*(x)=q_1^*(x)\cdots q_t^*(x),$$
其中对所有的 i 有 $p^*(x)=\Phi_j^*(p)$，$q_i^*(x)=\Phi_j^*(q_i)$. 注意到所有 $q_i^*(x)$是不可约的，因为同构将不可约多项式映为不可约多项式. 又因为 Φ_j 固定 k 的每一元，$p^*(x)=p(x)$. 由 $B[x]$中的唯一分解定理，$q_1^*(x)=q_\ell(x)$，对某 ℓ. 但 $z_j=\Phi_j(z_1)$是 $q_1^*(x)$的一个根，所以 $q_1^*(x)=q_j(x)$. 从而 $\deg(q_1)=\deg(q_1^*)=\deg(q_j)$，且所有 q_j 的次数都相同. ■

此引理使得我们能够刻画那些是某多项式的分裂域的域的扩张.

→ **定理 5.29** 设 E/k 是一个有限扩张，则 E/k 是$k[x]$中某多项式分裂域当且仅当$k[x]$中每一个在 E 中有一个根的不可约多项式在 $E[x]$中可分裂.

证明 假设 E/k 是 $k[x]$中某多项式的一个分裂域. 设 $p(x)\in k[x]$是不可约的，且设 $p(x)=q_1(x)\cdots q_t(x)$为 $E(x)$中的不可约多项式分解. 若 $p(x)$在 E 中有一个根，则它在 $E[x]$中有线性因式. 由引理 5.28，所有的 $q_i(x)$是线性的，故 $p(x)$在 $E[x]$中可分裂.

反之，假设 $k[x]$中的每一个在 E 中有一个根的不可约多项式在 $E[x]$中可分裂. 取 $\beta_1\in E$ 使得$\beta_1\notin k$. 因为 E/k 是有限的，所以由命题 3.116(i)，有一个以 β_1 为根的不可约多项式 $p_1(x)\in k[x]$. 由假设，$p_1(x)$在 $E[x]$中分裂. 设 $B_1\subseteq E$ 为 $p_1(x)$的一个分裂域. 若 $B_1=E$，则我们证毕. 否则取 $\beta_2\in E$ 且 $\beta_2\notin B_1$，与上面一样，存在以 β_2 为根的不可约多项式 $p_2(x)\in k[x]$. 定义 $B_2\subseteq E$ 为 $p_1(x)p_2(x)$的分裂域，这样 $k\subseteq B_1\subseteq B_2\subseteq E$. 因为 E/k 是有限的，所以此过程最终会终止，即存在某 $r\geqslant 1$ 使得 $E=B_r$. ■

→ **定义** 一个域扩张 E/k 称为是**正规扩张**，若每一个在 E 中有一个根的不可约多项式 $p(x)\in k[x]$在 $E[x]$中分裂.

为证明存在五次多项式没有类似于经典公式的那样的能给出它的根的公式，下面是我们的基本策略. 首先，我们将(给出 $f(x)\in k[x]$的根的)经典公式用 k 上分裂域 E 的子域的语言来叙述. 其次，这种用域的语言的叙述本身就是用群的语言的叙述：若 $f(x)$存在求根公式，则 $\mathrm{Gal}(E/k)$一定是可解群(其定义马上给出). 最后，次数不小于 5 的多项式具有不可解的伽罗瓦群.

→5.2.1 求根公式与根式可解性

不用进一步费力气，下面有一个多项式求根公式存在性的结论，它是用分裂域的子域的语

459 言来叙述的.

→ **定义** **型 m 的单纯扩张**指的是满足 $u^m\in k$ 的扩张 $k(u)/k$，其中 $m\geqslant 1$. 扩张 K/k 称为**根式扩张**若存在域塔
$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t=K \tag{2}$$
使得每个 K_{i+1}/K_i 都是单纯扩张. 我们称(2)为一个**根式塔**.

易见任何满足$[K:k]\leqslant 2$ 的域扩张 K/k 是一个单纯扩张. 由定理 4.54 可知，一个复数 z 是可构作的当且仅当它是多重 2 次的，也就是，存在一个域塔$\mathbb{Q}(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$ 使得 $z\in F_n$ 且对所有 i 有$[F_i:F_{i-1}]\leqslant 2$. 习题 5.17 要求证明$\mathbb{Q}(i,z)/\mathbb{Q}$ 为一个根式扩张.

当我们说存在一个类似于二次、三次、四次公式的求根公式时，我们的意思是说可以用

$f(x)$的系数表示出 $f(x)$的根. 同在经典公式中一样，这种表示牵涉到域的运算、常数及根的开方，但不涉及其他的运算，如余弦、定积分或取极限等. 当 $f(x)$为下面意义下的根式可解的时，上面非正式地描述的公式才能存在.

→ **定义** 设 $f(x)\in k[x]$有一个分裂域 E. 称 $f(x)$是**根式可解的**若存在根式扩张

$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t$$

使得 $E\subseteq K_t$.

→ **例 5.30** 对每一个域 k 和每一个 $m\geqslant 1$，我们来证明多项式 $f(x)=x^m-1\in k[x]$是根式可解的. 回忆到，由定理 3.55 可知在 $f(x)$的一个分裂域 E/k 中，所有 m 次单位根的集合 Γ_m 是一个循环群. 生成元 ζ 称为是一个本原单位根. 注意 $|\Gamma_m|=m$，除非 k 的特征为 $p>0$ 且 $p\mid m$，此时 $|\Gamma_m|=m'$，其中 $m=p^e m'$ 且 $p\nmid m'$[因为 $x^m-1=x^{p^e m'}-1=(x^{m'}-1)^{p^e}$]. 又 $E=k(\zeta)$，所以 E 是 k 的一个单纯扩张. 因此 E/k 是一个根式扩张，从而 $f(x)=x^m-1$ 是根式可解的. ◀

让我们通过分析低次多项式的经典公式来说明这个定义.

5.2.2 二次多项式

设 $f(x)=x^2+bx+c\in\mathbb{Q}[x]$. 定义 $K_1=\mathbb{Q}(u)$，其中 $u=\sqrt{b^2-4c}$，则 K_1 为$\mathbb{Q}$的根式扩张，因为 $u^2\in\mathbb{Q}$. 进一步，用二次求根公式可推出 K_1 为 $f(x)$的分裂域，所以 $f(x)$是根式可解的. 460

5.2.3 三次多项式

设 $f(X)=X^3+bX^2+cX+d\in\mathbb{Q}[x]$. 替换变量 $X=x-\frac{1}{3}b$ 就有新多项式 $f^*(x)=x^3+qx+r\in\mathbb{Q}[x]$，它们具有相同的分裂域[因为若 u 为 $f^*(x)$的一个根，则 $u-\frac{1}{3}b$ 为$f(x)$的一个根]. 定义 $K_1=\mathbb{Q}(\sqrt{D})$，其中 $D=r^2+4q^3/27$ 以及 $K_2=K_1(\alpha)$，其中 $\alpha^3=\frac{1}{2}(-r+\sqrt{D})$. 由三次求根公式，$K_2$ 包含 $f^*(x)$的根 $\alpha+\beta$，其中 $\beta=-q/3\alpha$. 最后定义 $K_3=K_2(\omega)$，其中 $\omega^3=1$. $f^*(x)$其余的根为 $\omega\alpha+\omega^2\beta$ 和 $\omega^2\alpha+\omega\beta$，它们均在 K_3 中，所以 $E\subseteq K_3$.

三次求根公式有一个有趣的情形，即所谓的不可约情形：一个$\mathbb{Q}[x]$中的三次不可约多项式，如果它的所有的根都是实数(如同像在例 5.6 中那样)，但用求根公式来表示其根的话，那么这些根需要用复数表示(见罗特曼(Rotman)著的《伽罗瓦理论》(Galois Theory)，第二版).

不可约情形 若 $f(x)=x^3+qx+r\in\mathbb{Q}[x]$是一个根全为实数的不可约多项式，则包含 $f(x)$的分裂域的任何根式扩张 $K_t/\mathbb{Q}$ 均不是实的，即 $K_t\nsubseteq\mathbb{R}$.

由此得出，我们不能修改 $f(x)$为根式可解的定义，使得 $f(x)$的分裂域 E 等于单纯扩张塔中的最后一项 K_t(以替代 $E\subseteq K_t$).

5.2.4 四次多项式

设 $f(x)=X^4+bX^3+cX^2+dX+e\in\mathbb{Q}[x]$. 改变变量 $X=x-\frac{1}{4}b$，得到新多项式 $f^*(x)=x^4+qx^2+rx+s\in\mathbb{Q}[x]$. 进一步，$f(x)$的分裂域等于 $f^*(x)$的分裂域，因为若 u 为 $f^*(x)$的一根，则 $u-\frac{1}{4}b$ 为 $f(x)$的一个根. 回忆到，

$$f^*(x) = x^4 + qx^2 + rx + s = (x^2 + jx + \ell)(x^2 - jx + m),$$

且(12)表明 j^2 为三次多项式

$$(j^2)^3 + 2q(j^2)^2 + (q^2 - 4s)j^2 - r^2.$$

的一个根. 同三次多项式情形一样，定义单纯扩张

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3,$$

故 $j^2 \in K_3$. 再定义 $K_4 = K_3(j)$，且注意到(11)式给出 ℓ, $m \in K_4$. 最后定义 $K_5 = K_4(\sqrt{j^2 - 4\ell})$, $K_6 = K_5(\sqrt{j^2 - 4m})$. 由四次求根公式有 $E \subseteq K_6$(此域塔可以被缩短).

我们已经看到二次、三次及四次多项式是根式可解的. 反过来，若 $f(x) \in \mathbb{Q}[x]$是一个根
461 式可解的多项式，则存在一个我们想得到的那种公式，它能用 $f(x)$的系数表示出 $f(x)$的根. 因为假设

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

是一个使得 $E \subseteq K_t$ 的根式扩张. 设 z 为 $f(x)$的一根. 又 $K_t = K_{t-1}(u)$，其中 u 为 K_{t-1}中某元素 $a \in K_{t-1}$的 m 次根. 因此 z 可以用 u 及 K_{t-1}中元素表示. 也就是说，z 可以用$\sqrt[m]{a}$及 K_{t-1}中元素表示. 但 $K_{t-1} = K_{t-2}(v)$，其中 v 的某次方幂属于 K_{t-2}. 因此 z 可以用 u，v 及 K_{t-2}中元素表示. 最终 z 可以用一个类似于那些经典公式的公式表示.

→5.2.5 用群论语言的叙述

这个策略的第二阶段就是研究 $f(x)$的根式可解性对它的伽罗瓦群的影响.

假设 $k(u)/k$ 是一个型 6 的单纯扩张，即 $u^6 \in k$. 因为$(u^3)^2 = u^6 \in k$，所以 $k(u^3)/k$ 是型 2 的单纯扩张. 显然，$k(u)/k(u^3)$是型 3 的单纯扩张. 因此 $k(u)/k$ 可用型 2 和 3 的单纯扩张塔 $k \subseteq k(u^3) \subseteq k(u)$来代替. 更一般地，对给定的一个单纯扩张塔，我们可以假设每一个域关于它的前一个域的单纯扩张都是素数型的：若 $k \subseteq k(u)$是型 m 的，则 $m = p_1 \cdots p_q$，其中各个 p_i 是素数(不必是不同的)，而 $k \subseteq k(u)$可替换为

$$k \subseteq k(u^{m/p_1}) \subseteq k(u^{m/p_1 p_2}) \subseteq \cdots \subseteq k(u).$$

下面是一个允许我们将根式可解转化为伽罗瓦群的语言的关键结果，同时也说明了正规扩张这个术语的来源. 读者应该认识到，域的扩张似乎与群的子群扮演同样的角色.

→ **定理 5.31** *设 $k \subseteq K \subseteq E$ 为一个域塔，其中 K/k，E/k 都是正规扩张. 则 $\mathrm{Gal}(E/K)$是 $\mathrm{Gal}(E/k)$的一个正规子群，且*

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/K) \cong \mathrm{Gal}(K/k).$$

证明 因为 K/k 是正规扩张，由定理 5.29，它是 $k[x]$中某多项式的一个分裂域. 因此若 $\sigma \in \mathrm{Gal}(E/k)$，那么由推论 5.19 可知 $\sigma(K) = K$. 规定 $\rho: \mathrm{Gal}(E/k) \to \mathrm{Gal}(K/k)$为 $\sigma \mapsto \sigma \mid K$. 同定理 5.21 的证明中一样，易见 ρ 是一个同态且 $\ker\rho = \mathrm{Gal}(E/K)$，从而 $\mathrm{Gal}(E/K)$就是 $\mathrm{Gal}(E/k)$的一个正规子群. 又 ρ 是一个满射：若 $\tau \in \mathrm{Gal}(K/k)$，应用命题 5.22(i)可知，存在扩展 τ 的 $\sigma \in \mathrm{Gal}(E/k)$，即 $\rho(\sigma) = \sigma | K = \tau$. 再由第一同构定理即完成证明. ■

462 在应用定理 5.31 时，需要下面这个(技术性的)引理.

引理 5.32 *设 B 为域 k 的一个有限扩张.*

(i)存在一个有限扩张 F/B 使得 F/k 为一个正规扩张.

(ii)若 B 是 k 的一个根式扩张，则存在一个域塔 $K\subseteq B\subseteq F$ 使得 F/k 既是一个正规扩张也是一个根式扩张．进一步，出现在 F/k 的根式塔的单纯扩张的型的集合与在 B/k 的根式塔的型的集合是一样的．

证明 (i)因为 B 是一个有限扩张，$B=k(z_1,\cdots,z_t)$，其中 $z_1,\cdots,z_t$ 为元素．对每一个 i，定理 3.116 给出不可约多项式 $p_i(x)\in k[x]$使得 $p_i(z_i)=0$．定义 $f(x)=p_1(x)\cdots p_t(x)\in k[x]\subseteq B[x]$，定义 F 为 $f(x)$在 B 上的一个分裂域．因为 $f(x)\in k[x]$，所以我们有 F/k 为 $f(x)$在 k 上的分裂域．从而 F/k 为一个正规扩张．

(ii)又

$$F=k(z_1,z_1',z_1'',\cdots;z_2,z_2',z_2'',\cdots;\cdots;z_t,z_t',z_t'',\cdots),$$

其中 z_i，z_i'，z_i''，…为 $p_i(x)$的根．我们断言

$$F=k(\{\sigma(z_1),\cdots,\sigma(z_t):\sigma\in \mathrm{Gal}(F/k)\}).$$

显然，右边包含在 F 中，故只须证明反包含成立．事实上，只须证明 $z_i'=\sigma(z_i)$[这里 z_i'现在表示 $p_i(x)$的任意一个根，对某 i]．由命题 3.116(iii)：存在确定的 k 的同构 $\gamma:k(z_i)\to k(z_i')$使得 $z_i\mapsto z_i'$．由命题 5.22(i)，每个这样的 γ 可扩展为一个同构 $\sigma\in\mathrm{Gal}(F/k)$．从而 $z_i'=\sigma(z_i)$．得证．

因为 B 是 k 的一个根式扩张，所以存在 $u_1,\cdots,u_t\in B$ 和一个根式塔，

$$k\subseteq k(u_1)\subseteq k(u_1,u_2)\cdots\subseteq k(u_1,\cdots,u_t)=B, \tag{3}$$

其中每个 $k(u_1,\cdots,u_{i+1})$都是 $k(u_1,\cdots,u_i)$的单纯扩张．我们现在来证明 F 为 k 的一个根式扩张．设 $\mathrm{Gal}(F/k)=\{\sigma_1=1,\sigma_2,\cdots,\sigma_n\}$．定义

$$B_1=k(u_1,\sigma_2(u_1),\sigma_3(u_1),\cdots,\sigma_n(u_1)).$$

存在根式塔

$$k\subseteq k(u_1)\subseteq k(u_1,\sigma_2(u_1))\subseteq k(u_1,\sigma_2(u_1),\sigma_3(u_1))\subseteq\cdots\subseteq B_1$$

它表明 B_1 为 k 的一个根式扩张．更详细地，若 u_1^p 落在 k 中，则 $\sigma_j(u_1^p)=\sigma_j(u_1)^p\in\sigma_j(k)=k\subseteq k(u_1,\sigma_2(u_1),\cdots,\sigma_{j-1}(u_1))$．注意这些单纯扩张的型都是一样的，即 p，也就是在根式域塔(3)中的型．规定

$$B_2=k(u_2,\sigma_2(u_2),\sigma_3(u_2),\cdots,\sigma_n(u_2));$$ 463

存在根式塔

$$B_1\subseteq B_1(u_2)\subseteq B_1(u_2,\sigma_2(u_2))\subseteq B_1(u_2,\sigma_2(u_2),\sigma_3(u_2))\subseteq\cdots\subseteq B_2.$$

又 B_2 为 B_1 的根式扩张：若 $u_2^q\in k(u_1)\subseteq B_1$，则 $\sigma_j(u_2^q)=\sigma_j(u_2)^q\in\sigma_j(B_1)\subseteq B_1\subseteq B_1(u_2,\sigma_2(u_2),\cdots,\sigma_{j-1}(u_2))$．同样，这些单纯扩张的型都是一样的，即 q，也就是在根式(3)中的型．因为 B_1 为 k 的一个根式扩张，k 至 B_1 的一个根式扩张跟着 B_1 至 B_2 的根式扩张推出 B_2 也是 k 的一个根式扩域．对每个 $i\geqslant 2$，规定 B_{i+1}为添加 u_i，$\sigma_2(u_i)$，$\sigma_3(u_i)$，…至 B_i 后而生成的子域．上述论断证明了 B_{i+1}为 k 的一个根式扩张．最后，因为 $F=B_t$，所以我们证明了 F 为 k 的一个根式扩张且关于单纯扩张的型论断也是成立的．■

→ **引理 5.33** 设 $k(u)/k$ 为一个型 p 的单纯扩张，p 与 k 特征不同．若 k 含有所有 p 次单位方根，且 $u\notin k$，则 $\mathrm{Gal}(k(u)/k)\cong \mathrm{I}_p$．

证明 记 $\mathrm{Gal}(k(u)/k)$为 G．设 $a=u^p\in k$．若 ω 为一个 p 次本原单位方根，则根 1，

ω，…，ω^{p-1}是不同的[因为 $p\neq \text{char}(k)$]，且 $f(x)=x^p-a$ 的根为 u，ωu，$\omega^2 u$，…，$\omega^{p-1}u$. 因为 $\omega\in k$，所以 $k(u)$是 $f(x)$在 k 上的一个分裂域. 若 $\sigma\in G$，那么由定理 5.18(i)，存在 i 使得$\sigma(u)=\omega^i u$. 定义 $\varphi: G\to \mathbb{I}_p$ 为 $\varphi(\sigma)=[i]$，mod p 的同余类. 先证 φ 为一个同态. 假设 $\tau\in G$ 且$\varphi(\tau)=[j]$，则 $\sigma\tau(u)=\sigma(\omega^j u)=\omega^{i+j}u$，所以 $\varphi(\sigma\tau)=[i+j]=[i]+[j]=\varphi(\sigma)+\varphi(\tau)$. 若 $\varphi(\sigma)=[0]$，则 $\sigma(u)=u$，所以 $\ker\varphi=\{1\}$. 因为由 G 的定义知道，σ 确定 k，命题 5.20 保证了 $\sigma=1$. 最后，我们证明 φ 为一个满射. 因为 $u\notin k$，自同构 $u\mapsto \omega u$ 不是恒等变换，所以 $\text{im}\varphi\neq\{[0]\}$. 但 p 阶群$\mathbb{I}_p$ 的子群只有$\{[0]\}$和$\mathbb{I}_p$，而 $\text{im}\varphi\neq\{[0]\}$，所以 $\text{im}\varphi=\mathbb{I}_p$，因此 φ 是一个同构. ■

下面是我们一直在寻找的用群论的语言表示的核心.

→ **定理 5.34** *设 $k=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\subseteq K_t$ 为域 k 的一个根式扩张. 假定对每个 i，K_i 是 K_{i-1}的素数 p_i 型的单纯扩张，其中 $p_i\neq\text{char}(k)$且 k 包含所有 p_i 次单位根.*

(i)若 K_t 是 k 上的一个分裂域，则存在子群列

$$\text{Gal}(K_t/k)=G_0\geqslant G_1\geqslant G_2\geqslant\cdots\geqslant G_t=\{1\},$$

使得每个 G_{i+1}是 G_i 的一个正规子群且G_i/G_{i+1}是素数阶循环群.

464 *(ii)若 $f(x)$根式可解，则它的伽罗瓦群 $\text{Gal}(E/k)$是一个可解群的商群.*

证明 (i)定义 $G_i=\text{Gal}(K_t/K_i)$给出 $\text{Gal}(K_t/k)$的一个子群链. 因为 $K_1=k(u)$，其中 $u^{p_1}\in k$，k 包含 p 次本原单位根的假设使得 K_1 为 $x^{p_1}-u^{p_1}$ 的一个分裂域(参见例 5.15). 应用定理 5.31 知 $G_1=\text{Gal}(K_t/K_1)$为 $G_0=\text{Gal}(K_t/k)$的一个正规子群，且 $G_0/G_1\cong\text{Gal}(K_1/k)/\text{Gal}(K_1/K_0)$. 由引理 5.33，$G_0/G_1\cong\mathbb{I}_{p_1}$. 对每个 i 重复以上论证，即得.

(ii)存在一个根式域塔

$$k=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\subseteq K_t,$$

其中每一个 K_i/K_{i+1}是素数型的单纯扩张且 $E\subseteq K_t$. 由引理 5.32，此根式域塔可以加长，即有根式域塔

$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t\subseteq\cdots\subseteq F,$$

其中 F/k 是一个正规扩张. 进一步，此更长的根式域塔的单纯扩张的(素数)型与出现在原来的根式域塔中的型是一样的. 因此在(i)中要求的 k 包含单位根的假设表明 $\text{Gal}(F/k)$为一个可解群.

因为 E 是一个分裂域，若 $\sigma\in\text{Gal}(F/k)$，则 $\sigma|E\in\text{Gal}(E/k)$，所以 $\rho:\sigma\mapsto\sigma|E$ 是一个同态 $\text{Gal}(F/k)\to\text{Gal}(E/k)$. 最后，命题 5.22(i)表明 ρ 是一个满射. 因为 F 是一个分裂域，所以每一个 $\sigma\in\text{Gal}(E/k)$可以扩展为某个 $\tilde{\sigma}\in\text{Gal}(F/k)$. ■

我们将看到不是每一个群都满足定理 5.34(i)的结论的，满足那样性质的群有一个名称.

→ **定义** *群 G 的***正规子群列***指的是如下形式的子群列*

$$G=G_0\geqslant G_1\geqslant G_2\geqslant\cdots\geqslant G_t=\{1\},$$

*其中 G_{i+1}为 G_i 的正规子群. 此子群列的***商群***是*

$$G_0/G_1,\quad G_1/G_2,\quad\cdots,\quad G_{t-1}/G_t.$$

*群 G 称为***可解的***，若 G 有一个使每个***商群***的阶均为素数的正规子群列.*

若依此的语言，定理 5.34 就是说：$\text{Gal}(K_t/k)$是一个可解群若 K_t 为 k 的一个根式扩张且

k 包含适当的单位方根. 465

→ **例 5.35** (i)S_4 是一个可解群.

考虑子群列

$$S_4 \geqslant A_4 \geqslant \mathbf{V} \geqslant W \geqslant \{1\},$$

其中 $\mathbf{V}$ 是四元群, W 为 $\mathbf{V}$ 的任意一个 2 阶群. 这是一个正规子群列: 首先从 S_4 开始, 至$\{1\}$结束; 其次, 每一项都是前一项的正规子群: $A_4 \lhd S_4$, $\mathbf{V} \lhd A_4$(事实上, 有更强的结论 $\mathbf{V} \lhd S_4$), $W \lhd \mathbf{V}$ 因为 $\mathbf{V}$ 是交换的. 又 $|S_4/A_4| = |S_4|/|A_4| = 24/12 = 2$, $|A_4/\mathbf{V}| = |A_4|/|\mathbf{V}| = 12/4 = 3$, $|\mathbf{V}/W| = |\mathbf{V}|/|W| = 4/2 = 2$ 和 $|W/\{1\}| = |W| = 2$, 因此每个商群都是素数阶的, 所以 S_4 是可解的.

(ii)每一个有限阿贝尔群 G 是可解的.

我们对 $|G|$ 进行归纳来证明此结论. 基础步骤 $|G| = 1$ 是平凡的. 对于归纳步, 回忆命题 2.124: 若 G 是一个有限阿贝尔群, 则对 $|G|$ 的每一个因子 d, G 有 d 阶的子群. 因为 $|G| > 1$, 所以对某素数 p 存在分解 $|G| = pd$, 从而存在 G 的 d 阶子群 H. 注意 $H \lhd G$, 因为 G 是阿贝尔群, 且 $|G/H| = |G|/|H| = pd/d = p$. 由归纳假设, 存在从$\{1\}$到 H 的正规子群列, 其商群是素数阶的. 由此得出 G 是一个可解群.

(iii)每一个非阿贝尔的单群 G 是不可解的.

因为 G 的仅有的正规子群为 G 和$\{1\}$, 所以 G 的每一个正规系列具有形式

$$G = G_0 = G_1 = \cdots = G_m > G_{m-1} = \cdots = G_t = \{1\}.$$

因此, 所有商群除了$\{1\}$外, 只能为 $G_m/G_{m-1} \cong G$. 因为 G 不是循环的(甚至不能是交换的), 所以 G 不是可解的.

(iv)S_5 不是一个可解群(事实上, 对所有 $n \geqslant 5$, S_n 不是一个可解群).

在习题 2.135 中我们看到, 对所有 $n \geqslant 5$, A_n 是 S_n 的唯一的真非平凡正规子群(证明中关键的之处是 $n \geqslant 5$ 时 A_n 是单群), 从而 S_n 只有唯一一个正规子群列, 也就是

$$S_n > A_n > \{1\}$$

(这不完全正确, 也有正规子群列 $S_n > A_n \geqslant A_n > \{1\}$, 其中有一项重复. 当然这种重复只是增加了一个新的商群 $A_n/A_n = \{1\}$). 但此正规子群列的商群为 $S_n/A_n \cong \mathbb{I}_2$ 和 $A_n/\{1\} \cong A_n$, 后一个群不是素数阶的. 因此对 $n \geqslant 5$, S_n 不是一个可解群. ◀ 466

→ **命题 5.36** *可解群 G 的每一个商群 G/N 也是可解的.*

注 可以证明, 可解群的每一个子群也都是可解的(参见本人所著的《高等近世代数》[⊖]中的命题 4.22). 因为 A_n 是单的, 由例 5.35(iii), 它是不可解的. 这就给出了当 $n \geqslant 5$ 时, S_n 是非可解的第二个证明.

证明 由群的第一同构定理知道群的商群同构于它的同态象, 所以只须证明, 若 $f: G \to H$ 是一个满同态(对某群 H), 则 H 为一个可解群.

设 $G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_t = \{1\}$ 为一个与可解群定义中一样的子群列, 则

$$H = f(G_0) \geqslant f(G_1) \geqslant f(G_2) \geqslant \cdots \geqslant f(G_t) = \{1\}$$

⊖ 本书中文版已由机械工业出版社出版——编辑注.

也是 H 的一个子群列. 若 $f(x_{i+1})\in f(G_{i+1})$ 且 $u_i\in f(G_i)$，则 $u_i=f(x_i)$ 且因为 $G_{i+1}\lhd G_i$，$u_i f(x_{i+1})u_i^{-1}=f(x_i)f(x_{i+1})f(x_i)^{-1}=f(x_ix_{i+1}x_i^{-1})\in f(G_i)$，即 $f(G_{i+1})$ 为 $f(G_i)$ 的一个正规子群. 由 $x_i\mapsto f(x_i)f(G_{i+1})$ 所规定的函数 $\varphi: G_i\to f(G_i)/f(G_{i+1})$ 是一个满射，因为它是满射 $G_i\to f(G_i)$ 和自然映射 $f(G_i)\to f(G_i)/f(G_{i+1})$ 的合成. 因为 $G_{i+1}\leqslant\ker\varphi$，此映射诱导了一个满同态 $G_i/G_{i+1}\to f(G_i)/f(G_{i+1})$，也就是 $x_iG_{i+1}\mapsto f(x_i)f(G_{i+1})$，由 G_i/G_{i+1} 为素数阶循环群可推出 $f(G_i)/f(G_{i+1})$ 为一个 1 阶群或素数阶循环群. 必要时去掉所有重复项即可得到 $H=f(G)$ 一个子群列，它的所有商群都是素数阶的循环群，所以 H 是一个可解群. ■

下面是主要的判别法则.

→ **定理 5.37(伽罗瓦)** *设 k 是一个域，$f(x)\in k[x]$. 若 k 包含了“足够多的”的单位根，$f(x)$ 是根式可解的，则它的伽罗瓦群 $\mathrm{Gal}(E/k)$ 是一个可解群.*

注 *设 E/k 是 $f(x)$ 的一个分裂域. 因为 $f(x)$ 是根式可解的，所以存在一个根式扩张 $k=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\subseteq K_t$ 使得每一个 $[K_{i+1}:K_i]$ 是素数且 $E\subseteq K_t$. 有“足够”的单位根的假设，我们的意思是 k 包含所有的 p 次单位根，这里 p 等于某些 $[K_{i+1}:K_i]$. 习题 5.28 表明如何去掉这个假设.*

证明 由引理 5.34(ii)，$\mathrm{Gal}(E/k)$ 是某个可解群的商群，且由命题 5.36 知，可解群的任何商群都是可解的，所以定理得证. ■

若 k 的特征为 0，则定理 5.37 的逆也成立，它也是由伽罗瓦证明(参见本人所著的《高等近
467 世代数》的第 235 页)的. 然而，当特征为 p 时，逆是不对的. 若 $f(x)=x^p-x-t\in k[x]$，其中 $k=\mathbb{F}_p(t)$，则 $f(x)$ 在 k 上的伽罗瓦群为 p 阶循环群. 但 $f(x)$ 不是根式可解的(参见《高等近世代数》中命题 4.56).

在 1827 年，阿贝尔证明了下面的定理：若多项式 $f(x)$ 的伽罗瓦群是交换群，则 $f(x)$ 是根式可解的. 这就是为什么将交换群称为阿贝尔群. 因为每一个有限阿贝尔群是可解的(参见例 5.35(ii))，所以阿贝尔定理是伽罗瓦定理的特殊情形.

证明 S_2，S_3 为 S_4 的每个子群都是可解的并不困难. 从而由定理 5.21 知，故每一个二次、三次及四次多项式的伽罗瓦群都是可解群. 因此由伽罗瓦定理的逆就知道，若 k 的特征为 0，则每一个满足 $\deg(f)\leqslant 4$ 的多项式 $f(x)$ 是根式可解的(当然我们早就知道了，因为我们已经证明了经典公式).

现在我们以证明，对于 $n\geqslant 5$ 一般 n 次多项式不是根式可解这一结论，从而来完成我们的讨论.

→ **定理 5.38(阿贝尔-鲁费尼)** *对所有的 $n\geqslant 5$，一般的 n 次多项式*

$$f(x)=(x-y_1)(x-y_2)\cdots(x-y_n)$$

不是根式可解的.

证明 设 F 为一个域，$E=F(y_1,\cdots,y_n)$ 是 F 上 n 个变量 $y_1,\cdots,y_n$ 的所有有理函数构成的域，且设 $k=F(a_0,\cdots,a_n)$，其中 a_i 是 $f(x)$ 的系数. 在习题 5.17 中我们看到，E 是 $f(x)$ 在 k 上的分裂域. 特别地，若我们选择 $F=\mathbb{C}$，则 k 为 $\mathbb{C}$ 的扩张，故它包含了所有的单位方根.

我们断言，S_n 同构于 $\mathrm{Gal}(E/k)$ 的一个子群. 习题 3.51(ii)说：若 A 和 R 为整环，$\varphi: A\to$

R 为同构映射，则 $a/b \mapsto \varphi(a)/\varphi(b)$ 是 $\mathrm{Frac}(A)\to\mathrm{Frac}(R)$ 的同构映射. 若 $\sigma\in S_n$，则由定理 3.33有 $f(y_1,\cdots,y_n)\mapsto f(y_{\sigma(1)},\cdots,y_{\sigma(n)})$ 就是 $\mathbb{C}[y_1,\cdots,y_n]$ 的一个固定 $\mathbb{C}$ 的自同构，当然，$\tilde{\sigma}$ 仅仅是置换多变量多项式中的变量. 由习题 3.51，整环 R 的自同构可以扩展为 $\mathrm{Frac}(R)$ 的自同构. 特别地，$\tilde{\sigma}$ 可扩展为 $E=\mathrm{Frac}(\mathbb{C}[y_1,\cdots,y_n])$ 的一个自同构 σ^*. 方程(1)显示 σ^* 确定 k，所以 $\sigma^*\in\mathrm{Gal}(E/k)$. 故应用命题 5.20，易见 $\sigma\mapsto\sigma^*$ 为 $S_n\to\mathrm{Gal}(E/k)$ 的一个单射，所以 $n!\leqslant|\mathrm{Gal}(E/k)|$. 但是由定理 5.21 知逆不等式也成立，所以 $n!=|\mathrm{Gal}(E/k)|$ 且 $\mathrm{Gal}(E/k)\cong S_n$. 因此当 $n\geqslant5$ 时，由例 5.35(iv)知 $\mathrm{Gal}(E/k)$ 不是一个可解群. 由定理 5.37 知 $f(x)$ 不是根式可解的. ■

我们已经证明了经典公式次数 $n\geqslant5$ 的多项式上的推广是不存在的. 468

→ **例 5.39** 下面是一个不能根式求解的 5 次多项式的直接的例子. 设 $f(x)=x^5-4x+2\in\mathbb{Q}[x]$. 由爱森斯坦因判别法(定理 3.102)，$f(x)$ 在 $\mathbb{Q}$ 上是不可约的. 设 $E/\mathbb{Q}$ 为 $f(x)$ 的包含在 $\mathbb{C}$ 中的分裂域，并且设 $G=\mathrm{Gal}(E/\mathbb{Q})$.

我们来用一些微积分. 导数 $f'(x)=5x^4-4$ 恰好有两个实根，即 $\pm\sqrt[4]{4/5}\sim\pm0.946$. 故 $f(x)$ 有两个临界点. 而 $f(\sqrt[4]{4/5})<0$，$f(-\sqrt[4]{4/5})>0$，故 $f(x)$ 有一个极大值和一个极小值. 易得出 $f(x)$ 恰有 3 个实根(尽管我们不需要知道它们的值，它们大约为 -1.5185，0.5085 和 1.2435；复根是 $-0.1168\pm1.4385i$). 记复共轭在 E 上的限制为 τ，则 τ 是一个轮换，因为 τ 对换两个复根而固定三个实根.

伽罗瓦群 G 同构于 $S_X\cong S_5$ 的一个子群，其中 X 是 $f(x)$ 的 5 个根的集合. 由推论 5.27 知 $|G|=[E:\mathbb{Q}]$ 被 5 整除，所以由柯西定理(定理 2.147)有 G 有 5 阶元 σ. σ 是一定是 5-循环，因为 S_5 中只有这样的 5 阶元. 习题 2.126 说 S_5 由任一个对换和任一个 5-循环生成，所以 $G=\mathrm{Gal}(E/\mathbb{Q})\cong S_5$. 由例 5.35(iv)，$\mathrm{Gal}(E/\mathbb{Q})$ 不是一个可解群，所以由定理 5.37(可去掉关于单位根的不必要的假设)可知 $f(x)$ 不是根式可解的. ◀

一个(不实用)的计算伽罗瓦群的算法在范德瓦尔登的《近世代数》(Modern Algebra)第 1 卷的第 189 页～192 页中给出，然而，伽罗瓦理论更多的进一步的结论是表明如何直接计算当 $\deg(f)\leqslant4$ 时 $f(x)\in Q[x]$ 的伽罗瓦群的.

习题

H 5.15 判别正误并给出理由.

(i)每一个代数闭域包含 n 个不同的 n 次单位根，其中 $n\geqslant1$.

(ii)在一个特征为 5 的域中，不存在 5 次单位根.

(iii)$\mathbb{R}$ 是 x^2-5 在 $\mathbb{Q}$ 上的一个分裂域.

(iv)$\mathbb{Q}(\sqrt{5})$ 是 $\mathbb{Q}$ 的一个正规扩张.

(v)$\mathbb{Q}[x]$ 中没有次数 $\geqslant5$ 的多项式是根式可解的.

(vi)$\mathbb{F}_2(x)=\mathrm{Frac}(\mathbb{F}_2[x])$ 是特征为 2 的无限域.

(vii)多项式 $f(x)\in\mathbb{Q}[x]$ 在 $\mathbb{C}$ 中可以有两个分裂域.

(viii)交错群 A_4 是一个可解群.

(ix)交错群 A_5 是一个可解群. 469

*5.16 设 $\varphi: A\to H$ 是一个群同态. 若 $B\lhd A$，$B\leqslant\ker\varphi$，试证由 $aB\mapsto\varphi(a)$ 给出的诱导映射 $\varphi^*: A/B\to H$ 是

一个定义良好的同态，且 $\mathrm{im}\varphi^* = \mathrm{im}\varphi$.

*5.17 若 $z \in \mathbb{C}$ 是一个可构造的数，试证 $\mathbb{Q}(i, z)/\mathbb{Q}$ 是一个根式扩张.

5.18 设 k 是一个域，$f(x) \in k[x]$，试证若 E 和 E' 是 $f(x)$ 在 k 上的分裂域，则 $\mathrm{Gal}(E/k) \cong \mathrm{Gal}(E'/k)$.

5.19 证明 $\mathbb{F}_3[x]/(x^3-x^2-1) \cong \mathbb{F}_3[x]/(x^3-x^2+x-1)$.

H5.20 $\mathbb{F}_4$ 是 $\mathbb{F}_8$ 的一个子域吗？

5.21 设 k 是特征为 $p>0$ 的一个域．定义**弗罗贝尼乌斯**(Frobenius)**映射** $F: k \to k$ 为 $F: a \mapsto a^p$.

(i)试证 $F: k \to k$ 是一个单同态.

H (ii)当 k 是有限域时，试证 F 是固定素域 $\mathbb{F}_p$ 的一个自同构，从而 $F \in \mathrm{Gal}(k/\mathbb{F}_p)$.

H (iii)试证：若 k 是有限域，则每个 $a \in k$ 有 p 次根，即存在 $b \in k$ 使得 $b^p = a$.

5.22 设 $q = p^n$，对某素数 p 和某 $n \geqslant 1$.

(i)若 α 为 $\mathbb{F}_q^{\times}$ 的一个生成元，试证 $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

H (ii)试证 α 的不可约多项式 $p(x) \in \mathbb{F}_p[x]$ 的次数为 n.

H (iii)试证若 $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$，则 $|G| \leqslant n$.

H (iv)试证 $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 是一个 n 阶循环群，弗罗贝尼乌斯映射 F 为它的一个生成元.

5.23 给定 $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$，试证下列论断是等价的.

(i) $f(x)$ 是不可约的.

(ii) $\sqrt{b^2-4ac}$ 不是一个有理数.

(iii) $\mathrm{Gal}(\mathbb{Q}(\sqrt{b^2-4ac})/\mathbb{Q})$ 的阶为 2.

*5.24 设 E/k 是多项式 $f(x) \in k[x]$ 的一个分裂域．若 $\deg(f) = n$，试证 $[E:k] \leqslant n!$．由此得出结论，E/k 是一个有限扩张.

H5.25 $x^{30}-1$ 在 $\mathbb{F}_5$ 上的分裂域的次数是多少？

5.26 试证，若 $f(x) \in \mathbb{Q}[x]$ 有有理根 a，则它的伽罗瓦群与 $f(x)/(x-a)$ 的伽罗瓦群相同.

*5.27 (i)设 H 为有限群 G 的一个正规子群．若 H 和 G/H 都是可解群，试证 G 是一个可解群.

(ii)若 H 和 K 是可解群，试证 $H \times K$ 也是可解群.

*5.28 我们去掉关于单位根的假设来证明定理 5.37：设 k 是一个域且 $f(x) \in k[x]$ 是根式可解的，则它的伽罗瓦群 $\mathrm{Gal}(E/k)$ 是一个可解群．因为 $f(x)$ 是根式可解的，所以存在一个根式域塔 $k = K_0 \subseteq \cdots \subseteq F$ 使得 $E \subseteq F$. 进一步，我们可以假设 F/k 是某多项式的一个分裂域．最后若 k 包含 m 次项单位根的一个特定集合 Ω，则 $\mathrm{Gal}(E/k)$ 是可解的.

(i)定义 E^*/E 是 x^m-1 的一个分裂域，定义 $k^* = k(\Omega)$．试证 E^* 是 $f(x)$ 在 k^* 上的一个分裂域．由此得出结论，$\mathrm{Gal}(E^*/k^*)$ 是可解的.

(ii)试证 $\mathrm{Gal}(E^*/k^*) \lhd \mathrm{Gal}(E^*/k)$ 且 $\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/k^*) \cong \mathrm{Gal}(k^*/k)$.

470 (iii)用习题 5.27 证明 $\mathrm{Gal}(E^*/k)$ 是可解的.

(iv)试证 $\mathrm{Gal}(E^*/E) \lhd \mathrm{Gal}(E^*/k)$ 且 $\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/E) \cong \mathrm{Gal}(E/k)$．由此得出结论，$\mathrm{Gal}(E/k)$ 是可解的.

*5.29 设 $f(x) \in \mathbb{Q}[x]$ 是一个不可约的 3 次多项式，其伽罗瓦群是 G.

H (i)证明：若 $f(x)$ 只有一个实根，则 $G \cong S_3$.

H (ii)求 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ 的伽罗瓦群.

H (iii)求一个三次多项式 $g(x) \in \mathbb{Q}[x]$ 使得它的伽罗瓦群是 3 阶的.

*5.30 (i)若 k 是一个域，$f(x) \in k[x]$ 的导数为 $f'(x)$．试证 $f'(x) = 0$ 或 $\deg(f') < \deg(f)$.

H (ii)若 k 是一个特征为 0 的域，试证不可约多项式 $p(x) \in k[x]$ 无重根，即，若 E 为 $p(x)$ 的分裂域，则

不存在 $a\in E$ 使得在 $E[x]$ 中 $(x-a)^2\mid p(x)$ 成立.

*5.31 设 k 为一个特征为 p 的域.

(i)试证，若 $f(x)=\sum_i a_ix^i\in k[x]$，则 $f'(x)=0$ 当且仅当 $f(x)$ 非零的系数仅仅是那些满足的 $p\mid i$ 的 a_i.

(ii)设 k 是有限的，$f(x)=\sum_i a_ix^i\in k[x]$. 试证 $f'(x)=0$ 当且仅当存在 $g(x)\in k[x]$ 使得 $f(x)=g(x)^p$.

(iii)试证，若 k 为一个有限域，则每一个不可约多项式 $p(x)\in k[x]$ 都无重根.

*5.32 H (i)若 $k=\mathbb{F}_p(t)$，$\mathbb{F}_p$ 上的有理函数构成的域，试证明 $x^p-t\in k[t]$ 有重根(可以证明，x^p-t 是一个不可约的多项式).

(ii)试证明 $E=k(\alpha)$ 是 x^p-t 在 k 上的一个分裂域.

(iii)试证 $\mathrm{Gal}(E/k)=\{1\}$.

5.3 结束语

这些思想的进一步研究就是伽罗瓦理论的主题了. 伽罗瓦理论研究扩域与它们的伽罗瓦群的关系. 除了它内在的美丽外，伽罗瓦理论被广泛地应用于代数数论中.

下列技术的记号被证明是重要的.

定义 多项式 $f(x)\in k[x]$ 称为是**可分的**，若它的不可约因式无重根(也就是，一个不可约多项式是可分的若它无重根). 有限域扩张 E/k 是**可分的**若每一个 $\alpha\in E$ 是 $k[x]$ 中一个无重根的不可约多项式的根.

我们看到，若 E 的特征为 0 或 E 为有限的，则 E/k 是可分的[习题 5.30(ii)，习题 5.31(iii)]. 另一方面，像我们在习题 5.32 中看到的一样，存在函数域 $\mathbb{F}_p(x)$ 的扩张是不可分的. 定理 5.26 的下面的推广表明了为什么可分多项式是有趣的(在本人所著的《高等近世代数》的定理 4.7 中有证明). 471

定理 设 k 是一个域，$f(x)\in k[x]$ 是可分的多项式. 若 E/k 是 $f(x)$ 的一个分裂域，则 $|\mathrm{Gal}(E/k)|=[E:k]$.

证明 定理 5.26 中的特征为 0 的假设仅仅是为了保证可分性. ■

定义 设 E/k 为一个域扩张，其伽罗瓦群为 $G=\mathrm{Gal}(E/k)$. 若 $H\leqslant G$，则**固定域** E^H 定义为

$$E^H=\{对所有的\ \sigma\in H, u\in E:\sigma(u)=u\}.$$

可以证明下列定理(例如，参见本人所著的《高等近世代数》的第 4.2 节). 刻画了分裂域的特征的定理 5.29 可以修改成用可分性来表达.

定理 设 E/k 为一个域扩张，其伽罗瓦群为 $G=\mathrm{Gal}(E/k)$. 则下列命题等价.

(i) E 是某可分多项式 $f(x)\in k[x]$ 的一个分裂域.

(ii)有一根属于 E 的不可约多项式 $p(x)\in k[x]$ 是可分的，$p(x)$ 在 $E[x]$ 中分裂.

(iii) $k=E^G$，即，对所有的 $\sigma\in G$，若 $a\in E$，$\sigma(a)=a$，则 $a\in k$.

定义 一个域扩张 E/k 叫做**伽罗瓦扩张**，若它满足上面定理中的任一个条件.

下面这个定理表明，在伽罗瓦扩张 E/k 的中间域 B(即满足 $k\subseteq B\subseteq E$ 的子域)与伽罗瓦群

的子群之间存在着密切的联系.

定理(伽罗瓦理论基本定理)　设 E/k 为一个有限伽罗瓦扩张，其伽罗瓦群为 $G=\mathrm{Gal}(E/k)$.

(i)函数 $H\mapsto E^H$ 是所有中间域构成的集合到 $\mathrm{Gal}(E/F)$ 的所有子群构成的集合的一个双射，并且此双射保持反包含关系：

$$H\leqslant L \text{ 当且仅当 } E^L\subseteq E^H.$$

对每个中间域 B 和每个子群 $H\leqslant G$，有下列成立

$$E^{\mathrm{Gal}(E/B)}=B \text{ 且 } \mathrm{Gal}(E/E^H)=H.$$

(ii)对每个中间域 B 和每个子群 $H\leqslant G$，有下列成立

472 $$[B:k]=[G:\mathrm{Gal}(E/B)] \text{ 且 } [G:H]=[E^H:k].$$

(iii)中间域 B 是 k 的伽罗瓦扩张当且仅当 $\mathrm{Gal}(E/B)$ 为 G 的正规子群.

下面给出一些推论.

定理(本原元定理)　若 E/k 为一个有限可分扩张，则存在**本原元** $\alpha\in E$，也就是 $E=k(\alpha)$.

特别地，$\mathbb{Q}$ 的每一个有限扩张都有本原元. 这是由施特尼兹(E. Steinitz)的一个定理可得. 施特尼兹定理说，给定一个有限扩张 E/k，存在 $\alpha\in E$ 使得 $E=k(\alpha)$ 当且仅当仅存在有限多个中间域 $k\subseteq B\subseteq E$. 而基本定理说，中间域构成的集合到 $\mathrm{Gal}(E/k)$ 的所有子群构成的集合之间存在一个双射.

定理　对 n 的每一个因子 d，有限域 $\mathbb{F}_q$，其中 $q=p^n$，有且仅有一个阶为 p^d 的子域.

这是从 $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 是 n 阶循环群和命题 2.75 而得的：若 G 是 n 阶循环群，则对 n 的每一个因子 d，G 有唯一的 d 阶子群.

定理　若 E/k 为一个伽罗瓦扩张且它的伽罗瓦群是阿贝尔群，则其每一个中间域也是伽罗瓦扩张.

这是从伽罗瓦基本定理而得的，因为阿贝尔群的每一个子群是正规的.

代数基本定理证明有许多种，其中就有用伽罗瓦理论的证明(参见本人所著的《高等近世代数》的第 233 页).

定理(代数基本定理)　设 $f(x)\in\mathbb{C}[x]$ 不是常数，则 $f(x)$ 在 $\mathbb{C}$ 中有一根.

我们现在用伽罗瓦群理论的基本定理来完成第 4 章中关于可构作性的讨论.

回忆到 p 是一个费马素数若 p 有形式 $p=2^m+1$(此时 $m=2^t$，参见推论 3.103 的证明). 我们给出高斯定理的证明后结束本章. 高斯定理是说，若 p 是一个费马素数，则正 p-边形可用直尺圆规作出.

引理 5.40　设 E/k 为一个伽罗瓦扩张，其伽罗瓦群为 $G=\mathrm{Gal}(E/k)$. 对给定的子群 $G\geqslant H\geqslant L$，有

473 $$[E^L:E^H]=[H:L].$$

证明　因为 $H\mapsto E^H$ 是保反序的，所以有域塔

$$k=E^G\subseteq E^H\subseteq E^L\subseteq E$$

(我们有 $k=E^G$ 是因为 E/k 是一个伽罗瓦扩张). 定理 4.31 给出 $[E^L:k]=[E^L:E^H][E^H:k]$，所以由伽罗瓦理论的基本定理有

$$[E^L : E^H] = \frac{[E^L : k]}{[E^H : k]} = \frac{[G : L]}{[G : H]} = \frac{|G| / |L|}{|G| / |H|} = \frac{|H|}{|L|} = [H : L].$$ ■

定理 5.41(高斯) 设 p 为奇素数，正 p-边形是可构作的当且仅当 $p=2^m+1$，对某 $m\geqslant 0$.

证明 必要性在定理 4.60 中已证，在那里我们证明了当 $m>0$ 时，m 必须为 2 的方幂.

若 p 为素数，则 $x^p-1=(x-1)\Phi_p(x)$，其中 $\Phi_p(x)$为 p 次分圆多项式. p 次本原单位根 ζ 是 $\Phi_p(x)$的一个根，且$\mathbb{Q}(\zeta)$是 $\Phi_p(x)$在$\mathbb{Q}$上的一个分裂域. 因为 $\Phi_p(x)$是一个次数为 $p-1$ 的不可约多项式(推论 3.103)，所以我们有$[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1=2^m$. 由定理 5.26，我们有 $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|=2^m$. $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$作为一个 2-群，它有正规子群列

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_t = \{1\}$$

其中每个商群都是 2 阶的，也就是对所有 $i\geqslant 1$ 有$[G_{i-1}:G_i]=2$. 由伽罗瓦理论基本定理可知，存在子域塔

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = \mathbb{Q}(\zeta).$$

进一步，由引理 5.40 知，对所有 $i\geqslant 1$ 有$[K_i : K_{i-1}]=[G_{i-1}:G_i]=2$. 这就是说 ζ 是多重二次的，因此由定理 4.54 知，ζ 是可构作的. ■ 474

第6章　群Ⅱ

6.1　有限阿贝尔群

我们考虑有限阿贝尔群以继续群的研究．习惯上，这些群的运算记为加法．我们即将证明，每一个有限阿贝尔群都是某些(有限)多个循环群的直和．为此我们从考虑直和开始．

定义　两个阿贝尔群 S 和 T 的**外直和**指的是阿贝尔群 $S\times T$，其做基础的集合是 S 和 T 的笛卡儿积，运算规定如下：$(s,t)+(s',t')=(s+s',t+t')$.

例行的检验就可得出外直和为一个(阿贝尔)群．单位元为 $(0,0)$，(s,t) 的逆元为 $(-s,-t)$．例如，平面 $\mathbb{R}^2$ 关于向量加法是一个群，且 $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$.

定义　设 S 和 T 为阿贝尔群 G 的子群，称 G 为 S 和 T 的**内直和**，记为 $G=S\oplus T$，每一个 $g\in G$ 均可唯一地表示成 $g=s+t$，其中 $s\in S$ 和 $t\in T$.

若 S 和 T 是阿贝尔群 G 的子群，定义

$$S+T=\{s+t:s\in S,t\in T\}.$$

注意 $S+T$ 总是 G 的一个子群，因为它就是 $\langle S\cup T\rangle$，由 S 和 T 生成的子群(参见习题 6.5)．说 $G=S+T$ 就是意味着每一个 $g\in G$ 均可表示成 $g=s+t$，其中 $s\in S$ 和 $t\in T$．说 $G=S\oplus T$ 就是意味这样的表示唯一．

下面是命题 2.127 的加法版本．我们不必说 S 和 T 是正规子群，因为阿贝尔群的每一个
475 子群都是正规的．

命题 6.1　若 S 和 T 是阿贝尔群 G 的子群，则 $G=S\oplus T$ 当且仅当 $S+T=G$ 且 $S\cap T=\{0\}$.

证明　假设 $G=S\oplus T$．每一个 $g\in G$ 均可唯一地表示成 $g=s+t$，其中 $s\in S$ 和 $t\in T$．因此 $G=S+T$．若 $x\in S\cap T$，则 x 表示成 $s+t$ 的方式有两种：$x=x+0$ 和 $x=0+x$．因为表示是唯一的，所以我们一定有 $x=0$，从而 $S\cap T=\{0\}$.

反之，由 $G=S+T$ 可推出每一个 $g\in G$ 均可表示成 $g=s+t$，其中 $s\in S$ 和 $t\in T$．下面证明表示是唯一的．假设又有 $g=s'+t'$，其中 $s'\in S$，$t'\in T$．那么由 $s+t=s'+t'$ 可推出 $s-s'=t'-t\in S\cap T=\{0\}$．因此 $s=s'$，$t=t'$，得证．■

定义　阿贝尔群 G 的一个子群 S 称为是 G 的一个**直和项**若存在 G 的一个子群 T 使得 $G=S\oplus T$．也就是，$G=S+T$ 且 $S\cap T=\{0\}$．这样的子群 T 称为 S 的**补**.

注意 $S\times T$ 不等于 $S\oplus T$，因为 S 与 T 均不是 $S\times T$ 的子群，实际上它们甚至不是笛卡儿积的子集．这一点很容易证明．给定阿贝尔群 S 和 T，定义外直和 $S\times T$ 的子群 S^* 和 T^* 为

$$S^*=\{(s,0):s\in S\}\text{ 和 }T^*=\{(0,t):t\in T\}.$$

当然通过 $s\mapsto(s,0)$ 有 $S\cong S^*$，通过 $t\mapsto(0,t)$ 有 $T\cong T^*$．易见 $S\times T=S^*\oplus T^*$，因为 $(s,t)=(s,0)+(0,t)$，故 $S^*+T^*=S\times T$ 且 $S^*\cap T^*=\{(0,0)\}$．因此外直和可以看成(子群同构于 S 和 T 的)内直和．相反地，下面的结果表明一个内直和同构于一个外直和．

命题 6.2 若 S 和 T 是阿贝尔群 G 的两个子群，且 $G=S+T$. 若 $G=S\oplus T$(也就是 $S\cap T=\{0\}$)，则存在一个同构 $\varphi: S\oplus T\to S\times T$ 使得 $\varphi(S)=S^*$ 和 $\varphi(T)=T^*$.

证明 若 $g\in S\oplus T$，引理 6.1 是说 g 可以唯一地表示为 $g=s+t$. 故定义 $\varphi: S\oplus T\to S\times T$ 为 $\varphi(g)=\varphi(s+t)=(s, t)$. 表示的唯一性表明 φ 是一个定义良好的函数. 显然，$\varphi(S)=S^*$ 且 $\varphi(T)=T^*$. 我们来验证 φ 是一个同态. 若 $g'=(s', t')$，则 $(s, t)+(s', t')=(s+s', t+t')$，因此

$$\begin{aligned}\varphi(g+g') &= \varphi(s+s'+t+t')\\ &= (s+s', t+t')\\ &= (s,t)+(s',t')\\ &= \varphi(g)+\varphi(g').\end{aligned}$$ 476

若 $\varphi(g)=(s, t)=(0, 0)$，则 $s=0$，$t=0$ 且 $g=s+t=0$. 因此 φ 是单射. 最后，φ 是满射，因为若 $(s, t)\in S\times T$，则 $\varphi(s+t)=(s, t)$. ■

我们现在将讨论推广至直和项多于两个的情形.

定义 阿贝尔群 S_1，S_2，…，S_n 的**外直和**是阿贝尔群 $S_1\times S_2\times\cdots\times S_n$，它的底集为 S_1，S_2，…，S_n 的笛卡儿积，它的运算由下列公式给出

$$(s_1, s_2, \cdots, s_n)+(s_1', s_2', \cdots, s_n')=(s_1+s_1', s_2+s_2', \cdots, s_n+s_n').$$

例如，n 维欧氏空间 $\mathbb{R}^n$ 是 $\mathbb{R}$ 与自己的 n 重的外直和：$\mathbb{R}^n=\mathbb{R}\times\cdots\times\mathbb{R}$.

定义 设 S_1，…，S_n 为阿贝尔群 G 的子群，称 G 为它们的**内直和**，记为

$$G=S_1\oplus\cdots\oplus S_n,$$

若每一个 $g\in G$，存在唯一一个 $s_i\in S_i$ 使得 $g=s_1+\cdots+s_n$.

例 6.3 设 k 是一个域，$G=k^n$ 是 k 与自己的 n 重外直和. 像通常一样，设 e_1，…，e_n 是标准基，也就是 $e_i=(0, \cdots, 0, 1, 0, \cdots, 0)$，第 i 个坐标是 1 其余坐标为 0 的 n 元有序组. 若 V_i 是由 e_i 生成的一维子空间，也就是，$V_i=\{ae_i : a\in k\}$，则 k^n 是内直和 $k^n=V_1\oplus\cdots\oplus V_n$，因为每一个向量都可以唯一地表示为一个基的线性组合. ◀

我们现在证明外直和可以看成内直和. 设 S_1，S_2，…，S_n 为阿贝尔群，对每一个 i 定义

$$S_i^*=\{(0,\cdots,0,s_i,0,\cdots,0) : s_i\in S_i\}\subseteq S_1\times\cdots\times S_n;$$

也就是 S_i^* 由笛卡儿积中所有除第 i 个坐标外其余坐标全是零的 n 元有序组组成. 当然，S_i 和 S_i^* 是同构的，因为对所有 i，通过 $s_i\mapsto(0, \cdots, 0, s_i, 0, \cdots, 0)$. 我们来证明 G 是内直和.

$$G=S_1^*\oplus\cdots\oplus S_n^*.$$

若 $g=(s_1, \cdots, s_n)\in S_1\times\cdots\times S_n$，则

$$g=(s_1,0,\cdots,0)+(0,s_2,0,\cdots,0)+\cdots+(0,\cdots,0,s_n).$$

这样的表示是唯一的，因为若 $(s_1, \cdots, s_n)=(t_1, \cdots, t_n)$，则由 n 元有序组的相等的定义给出，对所有的 i 有 $s_i=t_i$. 477

如何将引理 6.1 推广至多个直和项情形呢？若阿贝尔群 G 由子群 S_1，S_2，…，S_n 生成，人们首先猜想 $G=S_1\oplus\cdots\oplus S_n$ 当且仅当对所有 $i\neq j$，$S_i\cap S_j=\{0\}$. 但我们现在只证明这个是不够的.

设 V 是域 k 上的一个 2-维向量空间，x 和 y 为一个基. 因此 $V=\langle x\rangle\oplus\langle y\rangle$. 易证子空间 $\langle x\rangle$，$\langle y\rangle$ 和 $\langle x+y\rangle$ 中任两个的交是 $\{0\}$. 另一方面，我们没有 $V=\langle x\rangle\oplus\langle y\rangle\oplus\langle x+y\rangle$，因为 0 在 $\langle x\rangle+\langle y\rangle+\langle x+y\rangle$ 中有两种表示，即，$0=0+0+0$ 和 $0=-x-y+(x+y)$.

我们来证明每一个内直和都同构于一个外直和. 下面是引理 6.1 和命题 6.2 的推广.

命题 6.4 设 $G=S_1+S_2+\cdots+S_n$，其中 S_i 为 G 的子群，也就是每一个 $g\in G$ 可表示为

$$g = s_1 + s_2 + \cdots + s_n,$$

其中对所有 i 有 $s_i\in S_i$. 则下列条件等价：

(i) $G=S_1\oplus S_2\oplus\cdots\oplus S_n$. 即，对每一个元素 $g\in G$，表示 $g=s_1+s_2+\cdots+s_n$ 是唯一的，其中对所有 i 有 $s_i\in S_i$.

(ii) 存在一个同构 $\varphi: G\to S_1\times S_2\times\cdots\times S_n$ 使得 $\varphi(S_i)=S_i^*$，对所有的 i.

(iii) 对每个 i，若我们定义 $G_i=S_1+S_2+\cdots+\widehat{S}_i+\cdots+S_n$，其中 $\widehat{S}_i$ 表示 S_i 项从和式中去掉，则对每一个 i 有 $S_i\cap G_i=\{0\}$.

证明 (i)⇒(ii). 若 $g\in G$，$g=s_1+\cdots+s_n$，则定义 $\varphi: G\to S_1\times\cdots\times S_n$ 为 $\varphi(g)=\varphi(s_1+\cdots+s_n)=(s_1,\ \cdots,\ s_n)$. g 表示的唯一性表明 φ 是定义良好的. 直接可以验证，φ 是一个同构且对所有 i 有 $\varphi(S_i)=S_i^*$.

(ii)⇒(iii). 若 $g\in S_i\cap G_i$，则 $\varphi(g)\in S_i^*\cap(S_1^*+\cdots+\widehat{S_i^*}+\cdots+S_n^*)$. 但是若 $\varphi(g)\in S_1^*+\cdots+\widehat{S_i^*}+\cdots+S_n^*$，则它的第 i 个坐标是 0. 若 $\varphi(g)\in S_i^*$，则它的第 j 个坐标是 0，对所有的 $j\neq i$. 因此 $\varphi(g)=0$. 因为 φ 是一个同构，从而 $g=0$.

(iii)⇒(i). 设 $g\in G$，且假设

$$g = s_1 + \cdots + s_n = t_1 + \cdots + t_n,$$

其中对所有的 i 有 s_i，$t_i\in S_i$. 注意对每一个 i，$s_i-t_i=\sum_{j\neq i}(t_j-s_j)\in S_i\cap(S_1+S_2+\cdots+\widehat{S}_i+$
478 $\cdots+S_n)=\{0\}$. 因此对所有的 i 有 $s_i=t_i$，所以表示 $g=\sum_i s_i$ 是唯一的. ■

记号 从现在开始，我们就用记号 $S_1\oplus\cdots\oplus S_n$ 表示任一种直和，内直和或外直和，因为于我们的直和几乎都是指内直和. 我们将记[⊖]

$$\bigoplus_{i=1}^{n} S_i = S_1 \oplus \cdots \oplus S_n.$$

记号 $G=\sum_{i=1}^{n}S_i$ 是 $G=S_1+\cdots+S_n=\langle S_1\cup\cdots\cup S_n\rangle$ 的简记. 因此若每一个 $g\in G$ 均可表示成 $g=\sum_i s_i$，$s_i\in S_i$，则 $G=\sum_i S_i$；若 $G=\sum_i S_i$ 且表示 $g=\sum_i s_i$ 是唯一的，则 $G=\bigoplus S_i$.

"一次一个素数"地分析群的结构是比较方便的.

⊖ 在本书的前一版的后续著作《高等近世代数》中，我将直和记为 $\sum_i S_i$. 现在我认为将直和记为 $\bigoplus_i S_i$（这也是当今常用的几个符号之一）和将 sum（由 $\bigcup_i S_i$ 生成的子群）记为 $\sum_i S_i$ 会更清楚些. 如果有机会重新写《高等近世代数》的话，我在那里也会采用这些记号.

定义 设 p 是一个素数，阿贝尔群 G 称为 **p-准素的**[⊖]若对每个 $a\in G$，存在 $n\geqslant 1$ 使得 $p^n a=0$.

定义 设 G 为一个阿贝尔群，则它的 **p-准素分支**为

$$G_p=\{a\in G: p^n a=0,\text{对某 } n\geqslant 1\}.$$

如果我们不特指素数 p，我们就说阿贝尔群 G 是准素的(而不是 p-准素的). 显然准素分支是一个子群. 但是在非阿贝尔群中这是不成立的. 例如，若 $G=S_3$，则 $G_2=\{(1),(12),(13),(23)\}$，它不是 S_3 的一个子群因为 $(12)(13)=(132)\notin G_2$.

定理 6.5(准素分解定理) (i)每个有限阿贝尔群 G 是它的 p-准素分支的直和：

$$G=\bigoplus_p G_p.$$

(ii)两个有限阿贝尔群 G 和 G' 是同构的当且仅当 $G_p\cong G'_p$，对每个素数 p. 479

证明 (i)设 $x\in G$ 为一个非零元，又令它的阶为 d. 由算术基本定理，存在不同的素数 p_1，…，p_n 及正整数 e_1，…，e_n 使得

$$d=p_1^{e_1}\cdots p_n^{e_n}.$$

对每个 i 记 $r_i=d/p_i^{e_i}$，则 $p_i^{e_i}r_i=d$，从而 $r_i x\in G_{p_i}$. 但 r_1，…，r_n 的 gcd d 为 1(d 的可能的素因数为 p_1，…，p_n，但因为 $p_i\nmid r_i$，故没有一个 p_i 为公因数). 因此存在整数 s_1，…，s_n 使得 $\sum_i s_i r_i=1$，所以

$$x=\sum_i s_i r_i x\in G_{p_1}+\cdots+G_{p_n}.$$

记 $H_i=G_{p_1}+G_{p_2}+\cdots+\widehat{G_{p_i}}+\cdots+G_{p_n}$. 由命题 6.4 知，只须证明若

$$x\in G_{p_i}\cap H_i,$$

则 $x=0$. 因为 $x\in G_{p_i}$，所以我们有 $p_i^{\ell}x=0$，对某 $\ell\geqslant 0$. 因为 $x\in H_i$，我们有 $ux=0$，其中 $u=\prod_{j\neq i}p_j^{g_j}, g_j\geqslant 0$. 但 p_i^{ℓ} 和 u 是互素的，所以存在整数 s 和 t 使得 $1=sp_i^{\ell}+tu$. 从而

$$x=(sp_i^{\ell}+tu)x=sp_i^{\ell}x+tux=0.$$

(ii)若 $f: G\to G'$ 为一个同态映射，则对每个素数 p 有 $f(G_p)\subseteq G'_p$，因为若 $p^{\ell}a=0$，则 $0=f(p^{\ell}a)=p^{\ell}f(a)$. 若 f 为一个同构映射，则 $f^{-1}: G'\to G$ 也为一个同构映射(所以对所有 p 有 $f^{-1}(G'_p)\subseteq G_p$). 所以每个限制 $f\mid G_p: G_p\to G'_p$ 为一个同构映射，其逆为 $f^{-1}\mid G'_p$.

反过来，若对所有 p 存在同构 $f_p: G_p\to G'_p$，则存在 $\varphi: \bigoplus_p G_p\to\bigoplus_p G'_p$ 的同构 $\sum_p a_p\mapsto\sum_p f_p(a_p)$. ■

记号 若 G 为一个阿贝尔群，m 为一个整数，则

$$mG=\{ma: a\in G\}.$$

易见 mG 是 G 的一个子群.

⊖ 在第 2 章中，我们称一个有限群 G 是一个 p-群若 $|G|$ 是 p 的方幂，且我们在习题 2.117 中证明了，一个有限群 G 是一个 p-群当且仅当每一个 $g\in G$ 的阶是 p 的方. 因此一个 p-准素的阿贝尔群 G 就是一个阿贝尔 p-群. 若我们是在阿贝尔群中讨论，像我们现在这样，则用术语“p-准素的”；若我们是在一般群中讨论，则通常用术语“p-群”.

下面类型的子群将起到十分重要的作用.

定义 设 p 为一个素数，G 为一个 p-准素阿贝尔群[⊖]. 子群 $S\subseteq G$ 称为一个**纯子群**[⊜]若对所有 $n\geqslant 0$ 有

480

$$S\cap p^nG=p^nS.$$

对每个子群 $S\subseteq G$，包含关系 $S\cap p^nG\supseteq p^nS$ 总是成立的，因此上式中仅有反包含 $S\cap p^nG\subseteq p^nS$ 才有意义. 也就是说，若 $s\in S$ 满足方程 $s=p^ng$，对某 $g\in G$，则存在 $s'\in S$ 使得 $s=p^ns'$. 即，若方程 $s=p^nx$ 有对 $x\in G$ 的解，则此方程对 $x\in S$ 也有解.

例 6.6 (i)G 的每个直和项 S 都是一个纯子群. 若 $G=S\oplus T$ 且 $s=p^ng$，其中 $s\in S$ 和 $g\in G$. 注意 $g=u+v$，其中 $u\in S$ 和 $v\in T$，故 $s=p^nu+p^nv$. 因此 $p^nv=s-p^nu\in S\cap T=\{0\}$，所以 $p^nv=0$. 从而 $s=p^nu$ 且 S 是 G 的纯子群.

(ii)若 $G=\langle g\rangle$为 p^2 阶的循环群，其中 p 为一个素数，则 $S=\langle pg\rangle$不是 G 的一个纯子群. 每一个元素 $s'\in S$ 具有形式 $s'=mpg$，对某 $m\in\mathbb{Z}$. 又 $s=pg\in S$，若存在一元素 $s'\in S$ 使得$s=ps'$，则 $s=ps'=p(mpg)=mp^2g=0$，矛盾. ◀

在习题 6.12 中，我们将看到例 6.6(i)的逆是成立的：若 G 是一个有限阿贝尔群，S 为 G 的一个子群，则 S 是一个纯子群当且仅当 S 是一个直和项. 这就是我们引入纯子群原因，因为通过验证一些方程可解来证明 S 是一个直和项比构造一个子群 T 使得 $S+T=G$ 和 $S\cap T=\{0\}$ 容易些.

引理 6.7 若 p 为素数，G 是一个有限 p-准素阿贝尔群，则 G 有非零纯循环子群.

证明 设 $G=\langle x_1,\cdots,x_q\rangle$. 因为 G 是 p-准素的，所以对所有 i，x_i 的阶为 p^{n_i}. 若 $x\in G$，则 $x=\sum_i a_ix_i$，其中 $a_i\in\mathbb{Z}$，所以若 ℓ 为这些 n_i 中的最大者，则 $p^\ell x=0$. 现在选一个阶为 p^ℓ 的元素 $y\in G$(例如，y 可能为这些 x_i 中的某一个). 下面来证明 $S=\langle y\rangle$就是 G 的一个纯子群.

假设 $s\in S$ 使得 $s=mp^ty$，其中 $t\geqslant 0$ 且 $p\nmid m$. 又令

$$s=p^na,$$

对某 $a\in G$. 若 $t\geqslant n$，则定义 $s'=mp^{t-n}y\in S$. 这样

$$p^ns'=p^nmp^{t-n}y=mp^ty=s.$$

若 $t<n$，则

$$p^\ell a=p^{\ell-n}p^na=p^{\ell-n}s=p^{\ell-n}mp^ty=mp^{\ell-n+t}y.$$

但 $p\nmid m$ 且 $\ell-n+t<\ell$，因为 $-n+t<0$. 因此 $p^\ell a\neq 0$. 这与 y 为最大阶的元相违，故这种情形

481 不会出现. 因此 S 就是 G 的一个纯子群. ∎

命题 6.8 若 G 是一个阿贝尔群，p 是一个素数，则 G/pG 是$\mathbb{F}_p$ 上的一个向量空间. 且当 G 是有限群时，它是有限维的.

证明 若$[r]\in\mathbb{F}_p$，$a\in G$，则定义纯量乘法为

$$[r](a+pG)=ra+pG.$$

⊖ 若 G 不是一个准素群，则纯子群 $S\subseteq G$ 定义为满足 $S\cap mG=mS$ 的子群，对所有 $m\in\mathbb{Z}$(参阅习题 5.1 和 5.2).

⊜ 一个多项式方程称为纯的若它具有 $x^n=a$ 的形式. 纯子群是用这种方程的形式来命名的，这也许就是此称呼的来由.

这个运算是定义良好的，因为若 $k\equiv r \bmod p$，则对某整数 m 有 $k=r+pm$，这样

$$ka+pG=ra+pma+pG=ra+pG,$$

因为 $pma\in pG$. 同样的方法就可证明向量空间的公理成立. 若 G 是有限的，则 G/pG 是有限的. 显然 G/pG 具有有限基. ■

定义 若 p 是一个素数，G 是一个有限的 p-准素阿贝尔群，则

$$d(G)=\dim(G/pG).$$

注意到 d 在直和上是可加的，

$$d(G\oplus H)=d(G)+d(H),$$

因为由命题 2.126 知

$$\frac{G\oplus H}{p(G\oplus H)}=\frac{G\oplus H}{pG\oplus pH}\cong\frac{G}{pG}\oplus\frac{H}{pH}.$$

因为 G/pG 的一个基并上 H/pH 的一个基即为 $(G/pG)\oplus(H/pH)$ 的一个基，所以上式左边的维数为 $d(G\oplus H)$，右边的维数为 $d(G)+d(H)$.

$d(G)=1$ 的阿贝尔群 G 比较容易刻画.

引理 6.9 若 G 为一个 p-准素阿贝尔群，则 $d(G)=1$ 当且仅当 G 为循环的.

证明 若 G 为循环群，则 G 的任何商群也是循环群. 特别地 G/pG 也是循环群，所以 $\dim(G/pG)=1$，$d(G)=1$.

反之，假设 $d(G)=1$，即 $G/pG\cong\mathbb{I}_p$. 因为 $\mathbb{I}_p$ 是一个单群，对应定理告诉我们 pG 是 G 的极大子群. 下面证明 pG 是 G 的唯一的极大子群. 若 $L\subseteq G$ 是任一个极大子群，因为 G/L 是阶为 p 的方幂的阿贝尔单群，所以由命题 2.153 其阶为 p. 从而 $G/L\cong\mathbb{I}_p$. 因此，若 $a\in G$，在 G/L 中有 $p(a+L)=0$，即有 $pa\in L$，从而 $pG\subseteq L$. 但 pG 为极大的，所以 $pG=L$. 由此得出 G 的每个真子群都包含于 pG 中(因为每个真子群都包含于某极大子群中). 注意 $G/pG\cong\mathbb{I}_p$ 是循环的. 设对某 $z\in G$ 有 $G/pG=\langle z+pG\rangle$. 若 $\langle z\rangle$ 是 G 的一个真子群，则 $\langle z\rangle\subseteq pG$($G$ 的唯一的极大子群)，则与 $z+pG$ 为 G/pG 的一个生成元矛盾，所以 $G=\langle z\rangle$，从而 G 是循环的. ■ [482]

若 $G=(\mathbb{I}_p)^n$，则 $pG=\{0\}$，$G/pG\cong G$，且 $d(G)=\dim(G)$. 更一般地，若 G 是 p-准素循环群的直和，如 $G=\bigoplus_i C_i$，则 $pG=\bigoplus_i pC_i$. 由命题 2.126 有

$$G/pG=\Big(\bigoplus_i C_i\Big)\Big/\Big(\bigoplus_i pC_i\Big)\cong\bigoplus_i(C_i/pC_i).$$

我们刚刚看到对所有的 i 有 $d(C_i)=1$. 因此 d 在直和上的可加性表明 $d(G)$ 计算出 G 的分解中的循环直和项的数量.

引理 6.10 设 G 为一个有限 p-准素阿贝尔群.

(i) 若 $S\subseteq G$，则 $d(G/S)\leqslant d(G)$.

(ii) 若 S 为 G 的一个纯子群，则

$$d(G)=d(S)+d(G/S).$$

证明 (i) 由对应定理，$p(G/S)=(pG+S)/S$，所以由第三同构定理有

$$(G/S)/p(G/S)=(G/S)/[(pG+S)/S]\cong G/(pG+S),$$

因为 $pG \subseteq pG+S$，所以存在($\mathbb{F}_p$ 上向量空间的)满同态

$$G/pG \to G/(pG+S),$$

也就是 $g+pG \mapsto g+(pG+S)$. 因此 $\dim(G/pG) \geqslant \dim(G/(pG+S))$，即 $d(G) \geqslant d(G/S)$.

(ii)我们现在来分析$(pG+S)/pG$，它是映射 $G/pG \to G/(pG+S)$的核. 由第二同构定理，

$$(pG+S)/pG \cong S/(S \cap pG).$$

因为 S 是一个纯子群，所以 $S \cap pG = pS$，因此

$$(pG+S)/pG \cong S/pS,$$

所以 $\dim[(pG+S)/pG] = d(S)$. 但是若 W 是有限维向量空间 V 的一个子空间，那么由习题 4.17 知，$\dim(V) = \dim(W) + \dim(V/W)$. 所以若 $V = G/pG$ 且 $W = (pG+S)/pG$，则有

$$d(G) = d(S) + d(G/S). \qquad \blacksquare$$

483 **定理 6.11(基定理)** *每一个有限阿贝尔群 G 是一些准素循环群的直和.*

证明 由准素分解定理(即定理 6.5)，我们可以假设 G 就是一个 p-准素群，p 是某素数(因为若每一个准素分支是准素循环群的直和，则 G 也是). 我们对 $d(G) \geqslant 1$ 归纳来证明 G 是某些循环群的直和. 基础步骤是容易的，因为引理 6.9 表明在这种情形下 G 一定是循环的.

下面证明归纳步. 我们从应用引理 6.7 去找一个非零的纯循环子群 $S \subseteq G$ 开始. 由引理 6.10 我们有

$$d(G/S) = d(G) - d(S) = d(G) - 1 < d(G).$$

由归纳假设，G/S 是某些循环群的直和，即

$$G/S = \bigoplus_{i=1}^{q} \langle \bar{x}_i \rangle,$$

其中$\bar{x}_i = x_i + S$.

设 $x \in G$ 且$\bar{x}$的阶为 p^ℓ，其中$\bar{x} = x+S$. 我们断言，存在 $z \in G$ 使得 $z+S = \bar{x} = x+S$ 且 z 的阶为$\bar{x}$的阶. 又 x 的阶为 p^n，其中 $n \geqslant \ell$. 而在 G/S 中，$p^\ell(x+S) = p^\ell \bar{x} = 0$，所以存在某$s \in S$ 使得 $p^\ell x = s$. 由纯性的假设，存在 $s' \in S$ 使得 $p^\ell x_i = p^\ell s'$. 若我们规定 $z = x - s'$，则 $z+S = x+S$且 $p^\ell z = 0$. 因此若在 G/S 中 $m\bar{x} = 0$，则 $p^\ell \mid m$，从而在 G 中有 $mz = 0$.

对每个 i，选择 $z_i \in G$ 使得 $z_i + S = \bar{x}_i = x_i + S$ 且 z_i 的阶为$\bar{x}_i$ 的阶. 令 $T = \langle z_1, \cdots, z_q \rangle$. 因为 G 是由 S 及这些 z_i 生成的，所以 $S+T=G$. 要证 $G = S \oplus T$，只要证 $S \cap T = \{0\}$. 若 $y \in S \cap T$，则 $y = \sum_i m_i z_i$，其中 $m_i \in \mathbb{Z}$. 又 $y \in S$，所以在 G/S 中 $\sum_i m_i \bar{x}_i = 0$. 因为这是一个直和，所以每一个 $m_i \bar{x}_i = 0$. 总之，对每一个 i，

$$-m_i \bar{x}_i = \sum_{j \neq i} m_j \bar{x}_j \in \langle \bar{x}_i \rangle \cap (\langle \bar{x}_1 \rangle + \cdots + \widehat{\langle \bar{x}_i \rangle} + \cdots + \langle \bar{x}_q \rangle) = \{0\}.$$

因此对所有的 i 有 $m_i z_i = 0$，所以 $y=0$.

最后，由 $G = S \oplus T$ 就有 $d(G) = d(S) + d(T) = 1 + d(T)$，所以 $d(T) < d(G)$. 由归纳假设，T 是循环群的直和，这样就完成定理的证明了. $\blacksquare$

两个有限阿贝尔群 G 和 G'何时同构？由基定理，这样的群是循环群的直和，因此人们第一个猜测就是如果 G 和 G'的同一类型的循环直和项的个数相同，则它们是同构的. 但这个希

望被定理 2.128 打碎了. 定理 2.128 说，若 m，n 是互质的素数，则 $\mathbb{I}_{mn}\cong\mathbb{I}_m\times\mathbb{I}_n$. 例如，$\mathbb{I}_6\cong\mathbb{I}_2\times\mathbb{I}_3$. 因此我们退一步，转为计数准素循环项的个数. 但是我们怎样来计数呢？如同在算术基本定理理论中一样，我们必须问，是否存在某种形式的唯一分解定理？ 484

在叙述下一个引理前，回忆到我们定义了

$$d(G)=\dim(G/pG).$$

特别地，$d(pG)=\dim(pG/p^2G)$，且更一般地，

$$d(p^nG)=\dim(p^nG/p^{n+1}G).$$

引理 6.12 设 G 为一个有限 p-准素阿贝尔群，其中 p 是一个素数. 令 $G=\bigoplus_j C_j$，其中每个 C_j 是循环的. 若 p^n 阶的直和项 C_j 的个数为 b_n，则存在某 $t\geqslant 1$ 使得

$$d(p^nG)=b_{n+1}+b_{n+2}+\cdots+b_t.$$

证明 设 B_n 为所有阶为 p^n(若有的话)的 C_j 的直和，则存在某个 t 使得

$$G=B_1\oplus B_2\oplus\cdots\oplus B_t$$

又因为对所有 $j\leqslant n$，$p^nB_j=\{0\}$，所以

$$p^nG=p^nB_{n+1}\oplus\cdots\oplus p^nB_t,$$

类似地

$$p^{n+1}G=p^{n+1}B_{n+2}\oplus\cdots\oplus p^{n+1}B_t.$$

由命题 2.126，$p^nG/p^{n+1}G$ 同构于

$$[p^nB_{n+1}/p^{n+1}B_{n+1}]\oplus[p^nB_{n+2}/p^{n+1}B_{n+2}]\oplus\cdots\oplus[p^nB_t/p^{n+1}B_t].$$

因为 d 在直和上是可加的，所以

$$d(p^nG)=b_{n+1}+b_{n+2}+\cdots+b_t.$$ ■

这些数 b_n 可以用 G 来描述.

定义 若 G 是一个有限 p-准素阿贝尔群，其中 p 为一个素数，则

$$U_p(n,G)=d(p^nG)-d(p^{n+1}G).$$

由引理 6.12，

$$d(p^nG)=b_{n+1}+\cdots+b_t$$

且

$$d(p^{n+1}G)=b_{n+2}+\cdots+b_t,$$

所以 $U_p(n,G)=b_{n+1}$. 485

定理 6.13 若 p 为一个素数，则在有限 p-准素阿贝尔群 G 的任两个循环群的直和的分解中，每种类型的循环直和项的个数相同. 更准确地，对每个 $n\geqslant 0$，阶为 p^{n+1} 的循环直和项的项数为 $U_p(n,G)$.

证明 由基定理，存在循环子群 C_i 使得 $G=\bigoplus_i C_i$. 由引理 6.12，对每个 $n\geqslant 0$，阶为 p^{n+1} 的 C_i 的个数为 $U_p(n,G)$，这是一个与 G 的循环直和分解无关的数. 因此若 $G=\bigoplus_j D_j$ 为 G 的另一个分解，其中每个 D_j 为循环的，则阶为 p^{n+1} 的 D_j 的个数也为 $U_p(n,G)$，命题得证. ■

推理 6.14 若 G，G' 为有限 p-准素阿贝尔群，则 $G\cong G'$ 当且仅当对所有 $n\geqslant 0$，$U_p(n,G)=$

$U_p(n, G')$.

证明 若 $\varphi: G \to G'$ 是一个同构映射，则对所有 $n \geq 0$ 有 $\varphi(p^n G) = p^n G'$. 因此它诱导出 $\mathbb{Z}_p$ 上向量空间之间的同构 $p^n G / p^{n+1} G \cong p^n G' / p^{n+1} G'$，对所有 $n \geq 0$. 因此它们的维数是一样的，也就是 $U_p(n, G) = U_p(n, G')$.

反过来，假设对所有 $n \geq 0$，$U_p(n, G) = U_p(n, G')$. 若 $G = \bigoplus_i C_i$ 且 $G' = \bigoplus_j C'_j$，其中 C_i 和 C'_j 为循环的，那么由引理 6.12，每一种类型的直和项的个数是相等的，因此要构造一个 $G \to G'$ 的同构是一件简单的事情. ■

定义 若 G 是一个 p-准素阿贝尔群，则 G 的**初等因子**指的是一些数 p^{n+1}，每一个重复 $U_p(n, G)$ 次.

若 G 是一个有限阿贝尔群，则 G 的**初等因子**就是 G 的所有准素分支的初等因子.

例如，阿贝尔群 $\mathbb{I}_2 \oplus \mathbb{I}_2 \oplus \mathbb{I}_2$ 的初等因子是(2，2，2). $\mathbb{I}_6$ 的初等因子是(2，3). $\mathbb{I}_2 \oplus \mathbb{I}_2 \oplus \mathbb{I}_4 \oplus \mathbb{I}_8$ 的初等因子是(2，2，4，8).

定理 6.15(有限阿贝尔群的基本定理) 两个有限阿贝尔群 G 和 G' 是同构的当且仅当它们有相同的初等因子，也就是，在 G 和 G' 的任两个准素循环群的直和分解中每个阶的直和项的项数相同.

证明 由准素分解定理，即定理 6.5(ii)，$G \cong G'$ 当且仅当对每个素数 p，它们的准素分支是同构的：$G_p \cong G'_p$. 由定理 6.13 可得此结论. ■

此节的结论可从有限阿贝尔群推广到**有限生成的**阿贝尔群. 一个阿贝尔群叫做**有限生成**
486 **的**，若存在有限个元素 $a_1, \cdots, a_n \in G$ 使得每一个 $x \in G$ 都是它们的一个线性组合：$x = \sum_i m_i a_i$，其中对所有 i 有 $m_i \in \mathbb{Z}$. 基定理可推广为：每一个有限生成阿贝尔群 G 是某些循环群的直和，它们中的任一个或者为有限准素群或者为无限循环群. 无限循环群的直和称为**自由阿贝尔群**. 因此每一个有限生成阿贝尔群是自由阿贝尔群和有限群的直和. 定理 6.15 可推广为：给定 G 的两个无限和准素循环群的直和分解，则在两个分解中，每种类型的循环直和项的数目是一样的. 对于那些不是有限生成的阿贝尔群来说，基定理不再是正确的. 例如，有理数构成的加法群 $\mathbb{Q}$ 就不是循环群的直和.

此节的证明可以推广以证明**乌厄姆(ulm)定理**，乌厄姆定理给出了所有没有无限阶元素的可数阿贝尔群的分类.

习题

H 6.1 判断对错并给出理由.

(i)若 G 是有限阿贝尔群，则 Aut(G)是阿贝尔群.

(ii)若 $G = C_1 \oplus \cdots \oplus C_n = C'_1 \oplus \cdots \oplus C'_m$，其中 C_i 和 C'_j 是循环 p-准素群，对某素数 p，则 $m = n$ 且重新编号后，$C_i = C'_i$，对所有 i.

(iii)若 G 为一个阶无平方因子的阿贝尔群，$G = C_1 \oplus \cdots \oplus C_n$ 且 $G = C'_1 \oplus \cdots \oplus C'_m$，其中 C_i 和 C'_j 是循环 p-准素群，对某素数 p，则 $m = n$ 且重新编号后，$C_i = C'_i$，对所有 i.

(iv)若 G 和 H 为同阶的阿贝尔群，$pG = \{0\}$ 且 $pH = \{0\}$，则 $G \cong H$.

(v)四元群 $\mathbf{V}$ 是 $\mathbb{F}_2$ 上的一个向量空间.

(vi)Z 的每一个子群都是纯的.

(vii)Q 的每一个子群都是纯的.

(viii)8 阶非同构的阿贝尔群有 5 种.

(ix)若 p, q 是不同的素数，则$\mathbb{I}_p \to \mathbb{I}_q$ 的同态有 p 个.

(x)每一个 p^5 阶的阿贝尔群可以由 5 个或更少的元素生成，其中 p 是一个素数.

6.2 试证一个准素循环群 G 是**不可分的**，即，不存在非零的子群 S 和 T 使得 $G=S\oplus T$.

6.3 设 $S\subseteq H\subseteq G$ 是阿贝尔群.

(i)若 S 是 G 的纯子群，则 S 是 H 的纯子群.

(ii)试证纯性是传递的：若 S 是 H 的纯子群，H 是 G 的纯子群，则若 S 是 G 的纯子群.

6.4 (i)举一个阿贝尔群 $G=S\oplus T$ 的例子，使得它有子群 A 且满足 $A\neq(S\cap A)\oplus(T\cap A)$.

(ii)假设 G 是一个阿贝尔群，$G=S\oplus T$. 若 H 是 G 的一个子群且满足 $S\subseteq H\subseteq G$，试证 $H=S\oplus(T\cap H)$. 487

*6.5 (i)假设 G 是一个(加法)阿贝尔群，X 是 G 的一个非空子集，试证，由 X 生成的子群$\langle X\rangle$是所有系数在Z中的 X 中的元素的线性组合构成的集

$$\langle X\rangle=\Big\{\sum_i m_ix_i:x_i\in X,m_i\in\mathbb{Z}\Big\}.$$

试将此习题与命题 2.79 作比较.

(ii)若 S 和 T 是 G 的子群，试证 $S+T=\langle S\cap T\rangle$.

6.6 (i)若 G 和 H 是有限阿贝尔群，试证对所有素数 p 和所有 $n\geqslant 0$ 有

$$U_p(n,\ G\oplus H)=U_p(n,\ G)+U_p(n,\ H),$$

H (ii)若 A，B 和 C 为有限阿贝尔群，试证 $A\oplus B\cong A\oplus C$ 可推出 $B\cong C$.

H (iii)若 A 和 B 为有限阿贝尔群，试证 $A\oplus A\cong B\oplus B$ 可推出 $A\cong B$.

6.7 若 n 为一个正整数，n 的一个**划分**指的是一列正整数 $i_1\leqslant i_2\leqslant\cdots\leqslant i_r$ 且满足 $i_1+i_2+\cdots+i_r=n$. 若 p 为一个素数，试证阶为 p^n 的阿贝尔群在同构意义下的个数等于 n 的划分的个数.

H 6.8 在同构意义下阶为 288 的阿贝尔群的个数有多少?

6.9 通过将有限阿贝尔群基本定理应用于 $G=\mathbb{I}_n$ 来证明算术基本定理.

***H** 6.10 若 G 为一个有限阿贝尔群，定义

$$\nu_k(G)=G\text{ 中阶为 }k\text{ 的元素的个数}.$$

试证两个有限阿贝尔群 G 和 G'是同构的当且仅当对所有整数 k 有 $\nu_k(G)=\nu_k(G')$. (此结论对于非阿贝尔群是不成立的：参见命题 6.29).

6.11 视Q 为一个加法阿贝尔群.

(i)试证Q 的每一个有限生成子群是循环的.

(ii)试证Q 不是有限生成的.

(iii)试证Q $\not\cong A\oplus B$，其中 A，B 是非零子群.

*6.12 **H** (i)设 S 是 p-准素阿贝尔群 G 的一个子群，$\pi: G\to G/S$ 是自然映射 $g\mapsto g+S$. 试证 S 是 G 的纯子群当且仅当每一个 $g+S\in G/S$ 有原象 $g'\in G$(即 $\pi(g')=g+S$)且 g 和 g'的阶相等.

(ii)试证 p-准素阿贝尔群 G 的一个子群 S 是 G 的纯子群当且仅当它是一个直和项(对无限阿贝尔群，此结论不成立.)

H 6.13 设 F 和 F'是自由阿贝尔群. 若 F 是 n 个无限循环群的直和，F'是 m 个无限循环群的直和，试证 $F\cong F'$当且仅当 $m=n$.

6.14 (i)若 $F=\langle x_1\rangle\oplus\cdots\oplus\langle x_n\rangle$是自由阿贝尔群，试证每一个 $z\in F$ 有唯一的表示式 $z=m_1x_1+\cdots+m_nx_n$，其

中 $m_i \in \mathbf{Z}$，对所有的 i. 称 x_1，…，x_n 为 F 的一个基.

(ii)设 $X = x_1$，…，x_n 为 F 的一个基. 试证，若 A 是任意一个阿贝尔群，a_1，…，a_n 是 A 中任意一个
488 元素表，则存在唯一的同态 $f: F \to A$ 使得 $f(x_i) = a_i$，对所有的 i.

6.15 设 p 是一个素数. 试证，若 G 是一个有限 p-准素阿贝尔群，则 G 的每一个子群是纯子群当且仅当 $pG = \{0\}$.

*6.16 令 G 为一个阿贝尔群，不必是准素的. 称子群 $S \subseteq G$ 为一个**纯子群**，若对所有 $m \in \mathbf{Z}$ 有 $S \cap mG = mS$. 证明，若 G 为一个 p-准素阿贝尔群，其中 p 是一个素数，则子群 $S \subseteq G$ 是刚才所定义的纯子群当且仅当 $S \cap p^n G = p^n S$，对所有 $n \geqslant 0$(这就是正文中的纯子群的定义).

6.17 设 p 是一个素数，G 是一个有限 p-准素阿贝尔群.

(i)试证 pG 是 G 的所有极大子群的交.

(ii)(**弗拉蒂尼**)试证每一个 $g \in pG$ 是**非生成元**：若 $G = \langle X, g \rangle$，即 G 由 $X \cup \{g\}$ 生成，对某子集 $X \subseteq G$，则 $G = \langle X, g \rangle$.

(iii)(**伯恩赛德**)试证 $d(G)$ 是 G 的一个最小生成集 X 中的元素个数，即 X 生成 G，没有 X 的真子集生成 G.

*6.18 设 G 为有可能是无限的阿贝尔群[⊖]定义 G 的**挠子群**[⊜] tG 为

$$tG = \{a \in G : a \text{ 的阶为有限的}\}.$$

(i)试证 tG 为 G 的一个纯子群(存在挠子群 tG 不是直和项的阿贝尔群 G，因此纯子群不一定是一个直和项).

(ii)试证 G/tG 是一个每个非零元都是无限阶元的阿贝尔群.

6.19 设 S^1 为**圆群**，即所有模为 1 的复数构成的加法群. 试证挠子群 $G = tS^1$ 是一个无限群，且它的每一个有限子群是循环的.

6.2 西罗定理

我们现在回到非阿贝尔群，故将运算符号用回原来的乘法记号. 有限非阿贝尔群的西罗(L. Sylow)定理类似于有限阿贝尔群的准素分解定理.

回忆到，一个群 G 叫做单的若 $G \neq \{1\}$ 且除 $\{1\}$ 及 G 本身外无其他正规子群. 在命题 2.78 中，我们看到阿贝尔单群就是素数阿贝尔群 $\mathbb{I}_p$. 在定理 2.83 中我们看到对所有 $n \geqslant 5$，A_n 是一个非阿贝尔单群. 事实上，A_5 是最小阶的非阿贝尔单群. 人们怎样证明阶小于 $60 = |A_5|$ 的群不是单的呢？习题 2.105 讲道，若 G 是一个阶为 $|G| = mp$ 的群，其中 p 是素数，$1 < m < p$，
489 则 G 不是单群. 这个习题证明了许多小于 60 的数不是单群所具有的阶数. 去除所有为素数方幂的数后(由习题 2.118，p-群肯定不是非阿贝尔单群)，剩下有可能为单群的阶的数是

12， 18， 24， 30， 36， 40， 45， 48， 50， 54， 56.

这个习题的解答要用到柯西定理. 柯西定理指出，G 有一个 p 阶的子群. 我们将看到，若 G 有

⊖ 若不是无限的阿贝尔群，则可能不是一个子群，第 2.3 节中有一个矩阵群的例，它包含了两个有限阶的元素，但是这两个元的乘积是无限阶的.

⊜ 此术语来自代数拓扑. 对每个空间 X，附加上一序列的阿贝尔群，称为同调群. 若 X 是“扭曲的”，则这些群中某些群含有有限阶的元素.

一个阶是 p^e 而不是 p 的子群，其中 p^e 是整除 $|G|$ 的 p 的最高次幂，则习题 2.105 可被推广，上面候选的数的清单将减短为 30，40 和 56.

第一本群论的专著是约当(C. Jordan)著的《Traités des substitutions et des Equations Algebriques》，出版于 1870 年(其中超过一半的内容是伽罗瓦理论，当时称为方程的理论). 在几乎同时，群论的三个基本定理被发现了，但这些结果要发表于约当的书上的话就太迟了. 在 1868 年，师林(E. Schering)证明了基定理：每一个有限阿贝尔群都是循环群的直和，且每一个循环群都是素数方幂阶的. 在 1870 年，克罗内克在不知道师林的证明的情况下，也证明了这个结论. 在 1878 年，弗罗贝尼乌斯(G. Frobenius)和施蒂克贝格(L. Stickelberger)证明了有限阿贝尔群的基本定理. 在 1872 年，西罗证明了，对每个有限群 G 及任一个素数 p，若 p^e 是能整除 $|G|$ 的最大的 p 的方幂，则 G 有 p^e 阶的子群.

回忆到，p-群指的是它的每一个元素的阶都是 p 的方幂的有限群 G. 等价地，G 的阶为 p^k，对某 $k\geqslant 0$. (当整个地在阿贝尔群范围中讨论时，同我们在上节中的做法一样，人们称 G 为 p-准素群.)

定义 设 p 为一个素数，有限群 G 的**西罗 p-子群**指的是 G 的最大的 p-子群 P.

最大的意思是：若 Q 是 G 的一个 p-子群且 $P\leqslant Q$，则 $P=Q$. 西罗 p-子群总是存在的. 事实上，我们来证明，若 S 为 G 的任一个 p-子群(也许 $S=\{1\}$)，则存在一个包含 S 的西罗 p-子群 P. 若不存在严格包含 S 的 p-子群，则 S 本身就是一个西罗 p-子群，否则存在一个 p-子群 P_1，满足 $S<P_1$. 若 P_1 为极大的，则它就是一个西罗 p-子群，得证. 否则存在某 p-子群 P_2 使得 $P_1<P_2$，因此 $|P_1|<|P_2|$. 这种产生更大更大的 p-子群的程序一定在有限步后结束，因为 $|G|$ 是有限的. 因此这个最大的 P_i 一定是一个西罗 p-子群.

例 6.16 设 G 是一阶为 $|G|=p^e m$ 的有限群，其中 p 是一个素数且 $p\nmid m$. 我们证明，若存在一个阶为 p^e 的子群 P，则 P 是 G 的一个西罗 p-子群. 若 Q 是一个 p-子群，且有 $P\leqslant Q\leqslant G$，则 $|P|=p^e \mid |Q|$. 但是若 $|Q|=p^k$，则 $p^k \mid p^e m$ 且 $k\leqslant e$，即 $|Q|=p^e$ 且 $Q=P$. ◀ 490

定义 设 H 为群 G 的一个子群，则 H 的一个**共轭**为 G 的具有下面形式的子群 $gHg^{-1}=\{ghg^{-1}: h\in H\}$，对某 $g\in G$.

共轭子群都是同构的：若 $H\leqslant G$，则 $h\mapsto ghg^{-1}$ 是 $H\to G$ 的单射，其象为 gHg^{-1}. 反之不成立：四元群 $\mathbf{V}$ 包含几个阶为 2 的子群，当然，它们是同构的. 但它们不可能是共轭的因为 $\mathbf{V}$ 是阿贝尔群. 另一方面，在 S_3 中，所有 2 阶子群都是共轭的的. 例如，$\langle(1\ 3)\rangle=g\langle(1\ 2)\rangle g^{-1}$ 其中 $g=(2\ 3)$.

下面来用群作用的思想，而且复习一下我们在第二章中讨论的轨道和稳定子的概念.

定义 设 X 是一个集合，G 是一个群，称 G **作用**在 X 上，若对每一个 $g\in G$，存在函数 $\alpha_g: X\to X$ 使得

(i) 对 $g,h\in G$，$\alpha_g\circ\alpha_h=\alpha_{gh}$；

(ii) $\alpha_1=1_X$，恒等函数.

定义 若 G 作用在 X 上且 $x\in X$，则 x 的**轨道**，记为 $\mathcal{O}(x)$，指的是 X 的子集

$$\mathcal{O}(x) = \{\alpha_g(x) : g \in G\} \subseteq X;$$

x 的**稳定子**，记为 G_x，指的是

$$G_x = \{g \in G : \alpha_g(x) = x\} \leqslant G.$$

一个群 G 共轭地作用于它的所有子群构成的集合 $X = \mathbf{Sub}(G)$ 上：若 $g \in G$，则 g 的作用是：$\alpha_g(H) = gHg^{-1}$，其中 $H \leqslant G$. 子群 H 的轨道由它的所有共轭组成. H 的稳定化子是 $\{g \in G : gHg^{-1} = H\}$，这个子群有一个称呼.

定义 设 H 为群 G 的一个子群，则 H 在 G 的**正规化子**指的是子群

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

读者可以证明 $H \lhd N_G(H)$，因此商群 $N_G(H)/H$ 有定义.

命题 6.17 设 H 是有限群 G 的一个子群，则 H 在 G 中的共轭的个数是 $[G : N_G(H)]$.

491 **证明** 这是定理 2.143 的特殊情形：轨道的长是稳定化子的指数. ■

引理 6.18 设 P 是有限群 G 的一个西罗 p-子群.

(i) P 的每个共轭也是 G 的一个西罗 p-子群.

(ii) $p \nmid |N_G(P)/P|$.

(iii) 若 $g \in G$ 的阶为 p 的某方幂且 $gPg^{-1} = P$，则 $g \in P$.

证明 (i) 若 $g \in G$，则 gPg^{-1} 是 G 的一个 p-子群. 若它不是一个极大的 p-子群，则存在 p-子群 Q 使得 $gPg^{-1} < Q$. 因此 $P < g^{-1}Qg$，与 P 的极大性矛盾.

(ii) 若 p 整除 $|N_G(P)/P|$，则柯西定理表明 $N_G(P)/P$ 包含了一个 p 阶元 gP，因此 $N_G(P)/P$ 包含了一个 p-阶的(循环)子群 $S^* = \langle gP \rangle$. 由对应定理(定理 2.123)，存在满足 $P \leqslant S \leqslant N_G(P)$ 的子群 S 使得 $S/P \cong S^*$. 这样 S 是 $N_G(P) \leqslant G$ 的一个严格包含 P 的 p-子群(由习题 2.99 可得)，这与 P 的极大性相矛盾. 因此 p 不整除 $|N_G(P)/P|$.

(iii) 由正规化子的定义，元素 g 在 $N_G(P)$ 中. 若 $g \notin P$，则陪集 gP 是 $N_G(P)/P$ 的一个非平凡元素且阶为 p 的某方幂，结合(ii)，就知道这与拉格朗日定理矛盾. ■

因为西罗 p-子群的共轭还是西罗 p-子群，因此让 G 以共轭的方式作用于西罗 p-子群的集合上是合理的.

定理 6.19(西罗) 设 G 为一个阶为 $p^e m$ 的有限群，其中 p 是一个素数且 $p \nmid m$. 设 P 是 G 的一个西罗 p-子群.

(i) 每一个西罗 p-子群都与 P 共轭；

(ii) 若存在 r 个西罗 p-子群，则 r 为 $|G|/p^e$ 的一个因数，且 $r \equiv 1 \bmod p$.

证明 设 $X = \{P_1, \cdots, P_r\}$ 为 P 的所有共轭构成的集合，其中记 P 为 P_1. 若 Q 为 G 的任一个西罗 p-子群，则 Q 共轭作用于 X 上：若 $a \in Q$，则

$$\alpha_a(P_i) = \alpha_a(g_i P g_i^{-1}) = a(g_i P g_i^{-1})a^{-1} = (ag_i)P(ag_i)^{-1} \in X.$$

由推论 2.144，任何轨道中元素的个数都是 $|Q|$ 的一个因数，也就是说，每一个轨道的长都是 p 的某方幂(因为 Q 是一个 p-群). 若存在长为 1 的轨道，则存在某 P_i 满足 $aP_ia^{-1} = P_i$，对所有 $a \in Q$. 由引理 6.18，对所有 $a \in Q$，有 $a \in P_i$，也就是，$Q \leqslant P_i$，但作为一个西罗 p-子群，Q 是 G 的一个极大的 p-子群，所以 $Q = P_i$. 当 $Q = P_1$ 时用此论断，我们看到除了那个仅

包含 P_1 的轨道的长为 1 外，其余轨道的长都是 p 的正方幂，所以我们得出结论 $|X|=r\equiv 1 \bmod p$. 492

假设存在某西罗 p-子群 Q，它不是 P 的一个共轭，因此对任意 i 有 $Q\neq P_i$. 我们再让 Q 作用于 X 上. 若存在长为 1 的轨道，例如 $\{P_j\}$，则同理可得 $Q=P_j$，与假设 $Q\notin X$ 相违. 因此不存在长为 1 的轨道，这就是说每一个轨道的长都是 p 的正方幂，从而 $|X|=r$ 就是 p 的倍数，即 $r\equiv 0 \bmod p$，这与同余式 $r\equiv 1 \bmod p$ 相违. 因此这样的 Q 不存在. 所以所有的西罗 p-子群都共轭于 P. 最后因为所有的西罗 p-子群都是共轭的，我们有 $r=[G:N_G(P)]$. 因此 r 是 $|G|=p^e m$ 的一个因子. 但是因为 $r\equiv 1 \bmod p$，所以 $(r, p)=1$，从而 $r\mid p^e m$ 推出 $r\mid m$，即 $r\mid |G|/p^e$. ■

推论 6.20 *有限群 G 有唯一的一个西罗 p-子群当且仅当它有一个正规的西罗 p-子群.*

证明 假设 G 的西罗 p-子群 P 是唯一的. 由于对每个 $a\in G$，共轭 aPa^{-1} 也是一个西罗 p-子群，由唯一性，$aPa^{-1}=P$，所以 $P\lhd G$.

反之，假设 P 是 G 的正规的西罗 p-子群. 若 Q 是 G 的任一个西罗 p-子群，则对某 $a\in G$，$Q=aPa^{-1}$. 但由 P 的正规性，$aPa^{-1}=P$，所以 $Q=P$. ■

下面这个结果给出了西罗 p-子群的阶.

定理 6.21(西罗) *若 G 是一个阶为 $p^e m$ 的有限群，其中 p 是一个素数且 $p\nmid m$，则 G 的每一个西罗 p-子群的阶为 p^e.*

证明 我们首先证明 $p\nmid[G:P]$. 注意

$$[G:P]=[G:N_G(P)][N_G(P):P].$$

上面第一个因子 $[G:N_G(P)]=r$ 是 P 在 G 中共轭的个数，我们已经知道 $r\equiv 1 \bmod p$，因此 p 不整除 $[G:N_G(P)]$. 第二个因子是 $[N_G(P):P]=|N_G(P)/P|$，由引理 6.18(ii)，它也是不被 p 整除. 因此由欧几里得引理，p 不整除 $[G:P]$.

对某 $k\leqslant e$，$|P|=p^k$，所以

$$[G:P]=|G|/|P|=p^e m/p^k=p^{e-k}m.$$

因为 p 不整除 $[G:P]$，我们一定有 $k=e$，也就是 $|P|=p^e$. ■

例 6.22 (i)若 G 是一个有限阿贝尔群，则 G 的西罗 p-子群就是 G 的 p-准素分支. 因为 G 是阿贝尔群，每个子群都是正规的，所以对每一个素数 p，存在唯一一个西罗 p-子群. 493

(ii)设 $G=S_4$，则 $|S_4|=24=2^3\cdot 3$. 因此 S_4 的西罗 2-子群的阶为 8. 我们在习题 2.96 中已经看到，S_4 包含了一个同构于 D_8 的子群，而 D_8 是由于一个正方形的所有对称构成. 西罗定理说所有 8 阶子群都是共轭的，因此所有 8 阶子群都同构于 D_8. 进一步，西罗 2-子群的个数 r 是 24 的一个因子，在模 2 下同余于 1，即 r 为 24 的奇因数. 因为 $r\neq 1$(见习题 6.21)，因此 S_4 恰好有 3 个西罗 2-子群. ◀

这里有上一个西罗定理的第二种证明，由维兰特(Wielandt)给出.

定理 6.23(=定理 6.21) *若 G 是一个阶为 $p^e m$ 的有限群，其中 p 是一个素数且 $p\nmid m$，则 G 有 p^e 阶的子群.*

证明 设 X 为 G 中元素个数恰为 p^e 的子集的集合，则 $|X|=\binom{n}{p^e}$. 由习题 1.72 知，

$p\nmid|X|$. 注意 G 作用于 X 上：对 $g\in G$，$B\in X$，规定 $\alpha_g(B)=gB$，其中 $gB=\{gb:b\in B\}$. 对每个 $B\in X$，若 p 整除 $|\mathcal{O}(B)|$，则 p 为 $|X|$ 的因子，因为由命题 2.142，X 是轨道的无交并. 因为 $p\nmid|X|$，所以存在子集 B 满足 $|B|=p^e$ 且 p 不整除 $|\mathcal{O}(B)|$. 设 G_B 为此子群 B 的稳定化子，那么由定理 2.143，$[G:G_B]=|\mathcal{O}(B)|$，所以 $|G|=|G_B|\cdot|\mathcal{O}(B)|$. 因为 $p^e\mid|G|$，而 $p\nmid|\mathcal{O}(B)|$. 反复应用欧几里得引理即能给出 $p^e\mid|G_B|$. 因此 $p^e\leqslant|G_B|$.

下面证明逆不等式. 选择元素 $b\in B$，定义一个函数 $\tau:G_B\to B$ 为 $g\mapsto gb$. 注意 $\tau(g)=gb\in gB=B$，因为 g 在 B 的稳定化子 G_B 中. 若 g，$h\in G_B$ 且 $h\neq g$，则 $\tau(h)=hb\neq gb=\tau(g)$，所以 τ 是一个单射. 因此 $|G_B|\leqslant|B|=p^e$，从而 G_B 就是 G 的一个阶为 p^e 的子群. ■

若 p 是一个不整除有限群 G 的阶的素数，则 G 的西罗 p-子群的阶为 $p^0=1$. 因此当我们说 G 的西罗 p-子群时，我们通常避免平凡的情形并假设 p 是 $|G|$ 的一个因子.

我们现在可以来推广习题 2.134 和它的解答.

引理 6.24 *不存在阶为 $p^e m$ 的非阿贝尔单群 G，其中 p 是一个素数，$p\nmid m$ 且 $p^e\nmid(m-1)!$.*

证明 假设这样的单群 G 存在. 由西罗定理，G 包含阶为 p^e 的子群 P，其在 G 中的指数为 m. 由定理 2.67，存在 G 在 P 的陪集上的表示，即存在同态 $\varphi:G\to S_m$ 满足 $\ker\varphi\leqslant P$. 然而，因为 G 是单的，所以它无真正规子群，因此 $\ker\varphi=\{1\}$，即 φ 为一个单射，即有 $G\cong\varphi(G)$
494 $\leqslant S_m$. 由拉格朗日定理，$p^e m\mid m!$，所以 $p^e\mid(m-1)!$，与假设矛盾. ■

引理 6.25 *不存在阶小于 60 的非阿贝尔单群.*

证明 若 p 是一个素数，习题 2.118 说每个满足 $|G|>p$ 的 p-群是非单的.

读者检验可发现，在 2 与 59 之间且不为素数方幂又没有如前面引理所叙述的分解 $n=p^e m$ 的整数 n 只有 30，40 及 56. 由前面的引理，只有这三个数才有可能成为阶<60 的非阿贝尔单群的阶.

假设有一个阶为 30 的单群 G. 设 P 为 G 的一个西罗 5-子群，故 $|P|=5$. P 的共轭的个数 r_5 为 $30/5=6$ 的因子且 $r_5\equiv1 \bmod 5$. 又 $r_5\neq1$，否则 $P\lhd G$. 故 $r_5=6$. 由拉格朗日定理，这些子群中的任两个的交是平凡的(西罗子群的交可以很复杂，见习题 6.22). 这些群中每一个都含有 4 个非单位元的元素，因此它们的并共有 $6\times4=24$ 个非单位元的元素. 类似地，G 的西罗 3-子群的个数 r_3 是 10(因为 $r_3\neq1$，r_3 是 30/3 的因子且 $r_3\equiv1 \bmod 3$)，每一个这样的群含有 2 个非单位元的元素，因此这些子群的并共含有 20 个非单位元的元素. 这两大类元素的个数已经超过了 G 中元素的个数，所以 G 不是单群.

假设 G 是阶为 40 的群，P 是 G 西罗 5-子群. 若 r_5 为 P 的共轭的个数，则 $r_5\mid 40/5$ 且 $r_5\equiv1 \bmod 5$. 这些条件导致 $r_5=1$，故 $P\lhd G$. 因此不存在阶为 40 的单群.

最后假设存在阶为 56 的单群 G. 若 P 为 G 的一个西罗 7-子群，则 P 一定有 $r=8$ 个共轭(因为 $r_7\mid 56/7$ 且 $r_7\equiv1 \bmod 7$). 因为这些群都是素数阶循环群，它们中任两个的交为 $\{1\}$，因此它们的并中共有 48 个非单位元的元素. 因此加上单位元，我们已经算了 G 的 49 个元素. 又一个西罗 2-子群 Q 的阶为 8，因此它又贡献了有另外 7 个非单位元的元素，这样我们已有了 56 个元素. 但是除非 $Q\lhd G$，否则还有另一个西罗 2-子群，这样元素个数就超过了限额. 因此

不存在阶为 56 的单群. ■

拉格朗日定理的"逆定理"是不成立的：设 G 是一个阶为 n 的有限群，若 $d \mid n$，则 G 可能没有 d 阶的子群. 例如，在命题 2.99 中，我们证明了 A_4 是一个 12 阶的群，但它没有 6 阶子群.

命题 6.26 *令 G 为一个有限群. 若 p 是一个素数且 p^k 整除 $|G|$，则 G 含有阶为 p^k 的子群.*

证明 设 $|G| = p^e m$，其中 $p \nmid m$，则 G 的西罗 p-子群的阶为 p^e. 因此若 p^k 整除 $|G|$，则 p^k 整除 $|P|$. 由命题 2.152，P 含有阶为 p^k 的子群，从而 G 更有理由含有阶为 p^k 的子群. ■

我们见过多少种 p 群？当然，阶为 p^n 的循环群是 p-群，这样的循环子群的直积也是 p-群. 由有限阿贝尔 p-群的基定理，它描述了所有有限阿贝尔群. 到目前为止，我们所见过的 495
非阿贝尔群只有二面体群 D_{2n}（当 n 为 2 的方幂时，它是一个 2-群）及阶为 8 的四元数群 $\mathbf{Q}$（当然，对每有个 2-群 A，直积 $D_8 \times A$ 及 $\mathbf{Q} \times A$ 也是非阿贝尔 2-群）和例 2.150 中的由所有 $\mathbb{F}_p$ 上具有形式 $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ 的上三角 3×3 矩阵构成的群 $\mathrm{UT}(3, p)$. $\mathrm{UT}(3, p)$ 明显的推广给出一族有趣的非阿贝尔 p-群.

定义 *设 k 为一个域，k 上的一个 $n \times n$ 的*单位三角*矩阵指的是主对角线上元素均为 1 的上三角矩阵. 用 $\mathrm{UT}(n, k)$ 表示 k 上所有 $n \times n$ 的单位三角矩阵构成的集合.*

命题 6.27 *对每个域 k，$\mathrm{UT}(n, k)$ 是 $\mathrm{GL}(n, k)$ 的一个子群.*

证明 若 $A \in \mathrm{UT}(n, k)$，则 $A = I + N$，其中 N 为严格上三角的，即 N 为主对角线上元素全为 0 的上三角矩阵. 注意严格上三角矩阵的和与积还是严格上三角矩阵.

令 $e_1, \cdots, e_n$ 为 k^n 的标准基. 设 N 为严格上三角的. 定义 $T: k^n \to k^n$ 为：$T(e_i) = Ne_i$，其中 e_i 被视为一个列矩阵. 对所有 i，T 满足下方程：

$$T(e_1) = 0 \text{ 且 } T(e_{i+1}) \in \langle e_1, \cdots, e_i \rangle.$$

易见，对 i 用归纳法可得 $T^i(e_j) = 0$，对所有 $j \leqslant i$. 从而 $T^n = 0$，这样 $N^n = 0$. 因此得出，若 $A \in \mathrm{UT}(n, k)$，则 $A = I + N$，其中 $N^n = 0$.

我们现在能够证明 $\mathrm{UT}(n, k)$ 是 $\mathrm{GL}(n, k)$ 的一个子群. 首先，若 A 是单位三角的，则它是非退化的. 类似于幂级数展开 $1/(1+x) = 1 - x + x^2 - x^3 + \cdots$，我们来看 $B = I - N + N^2 - N^3 + \cdots$ 是不是 $A = I + N$ 的逆矩阵（注意矩阵幂级数终止于第 $n-1$ 项，因为 $N^n = 0$），读者可以检验下式成立：$BA = I$. 因此 A 为非退化的. 进一步，因为 N 是严格上三角的，所以 $-N + N^2 - N^3 + \cdots$ 也是严格上三角的，从而 A^{-1} 是单位三角的. 最后，$(I+N)(I+M) = I + (N + M + NM)$ 是单位三角矩阵，所以 $\mathrm{UT}(n, k)$ 是 $\mathrm{GL}(n, k)$ 的一个子群. ■

命题 6.28 *设 $q = p^e$，其中 p 是一个素数，则对每个 $n \geqslant 2$，$\mathrm{UT}(n, \mathbb{F}_q)$ 是一个 p-群，阶为 $q^{n(n-1)/2}$.*

证明 在一个 $n \times n$ 的单位三角矩阵中，严格位于主对角线之上的元素共有 $\frac{1}{2}(n^2 - n) = n(n-1)/2$ 个. 因为这些元素可以为 $\mathbb{F}_q$ 中的任一个元素，因此 $\mathbb{F}_q$ 上的 $n \times n$ 的单位三角矩阵恰

496 好有 $q^{n(n-1)/2}$ 个，这就是 $UT(n, F_q)$ 的阶. ■

在习题 2.123 中，我们证明了 $UT(3, F_2) \cong D_8$.

回忆一下习题 2.44：若 G 为一个群且对所有 $x\in G$ 有 $x^2=1$，则 G 为阿贝尔群. 现在问：若 G 满足对所有 $x\in G$，$x^p=1$，其中 p 是一个素数，G 是否一定是阿贝尔群?

命题 6.29 设 G 为一个奇素数，则存在阶为 p^3 的非阿贝尔群 G，它满足对所有 $x\in G$，$x^p=1$.

证明 设 $G=UT(3, F_p)$，则 $|G|=p^3$. 若 $A\in G$，则 $A=I+N$，其中 $N^3=0$，因此 $N^p=0$ 因为 $p\geqslant 3$. 因为 $IN=N=NI$，二项式定理给出 $A^p=(I+N)^p=I^p+N^p=I$. ■

在习题 6.10 中，我们定义 $\nu_k(G)$ 为 G 中阶为 k 的元素的个数. 我们证明了若 G 和 H 为一个阿贝尔群且对所有整数 k，$\nu_k(G)=\nu_k(H)$，则 G 和 H 是同构的. 在一般情形下，此结论是不成立的，因为若 p 是一个奇素数，则 $UT(3, F_p)$ 和 $\mathbb{I}_p\times\mathbb{I}_p\times\mathbb{I}_p$ 都包含单位元和 p^3-1 个阶元.

定理 6.30 令 F_q 表示具有 q 个元素的有限域，则

$$|GL(n,F_q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}).$$

证明 令 V 是 F_q 上的一个 n 维向量空间. 我们首先证明存在一个双射 $\Phi: GL(n, F_q)\to \mathcal{B}$，其中 $\mathcal{B}$ 是 V 的所有基构成的集合. 在 V 的所有基中任取一个：$e_1, \cdots, e_n$. 若 $T\in GL(n, F_q)$，则定义 $\Phi(T)=Te_1, \cdots, Te_n$. 因为 T 是非退化的，由引理 4.77，T 将一个基映为一个基，所以 $\Phi(T)\in\mathcal{B}$. 因为对给定的一个基 $v_1, \cdots, v_n$，(由引理 4.77)存在唯一的非退化的线性变换 S，(由定理 4.62)使得对所有 i 有 $Se_i=v_i$，所以 Φ 是一个双射.

因此我们的问题归纳为计算 V 的基 $v_1, \cdots, v_n$ 的数量. V 中有 q^n 个向量，故意 v_1 有 q^n-1 个选择(不能选零向量). 取定 v_1 后，我们看到 v_2 不能选 v_1 张成的子空间 $\langle v_1\rangle$ 中的元素，故 v_2 有 q^n-q 种选择. 更一般地，取定一个线性无量的向量链 $v_1, \cdots, v_i$ 后，v_{i+1} 可为任何 $\langle v_1, \cdots, v_i\rangle$ 之外的向量，因此 v_{i+1} 有 q^n-q^i 种选择. 对 i 用归纳法即得出结论. ■

推理 6.31 $|GL(n, F_q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)(q-1)$.

证明 公式

$$|GL(n,F_q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$

497 中 q 的方幂为 $q^{1+2+\cdots+(n-1)}$，且 $1+2+\cdots+(n-1)=\frac{1}{2}n(n-1)$. ■

定理 6.32 若 p 是一个素数且 $q=p^m$，则单位三角群 $UT(n, F_q)$ 是 $GL(n, F_q)$ 的一个西罗p-子群.

证明 因为由推论 6.31 知，$|UT(n, F_q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)(q-1)$，所以整除 $|GL(n, F_q)|$ 的 p 的最高次幂是 $q^{n(n-1)/2}$，而 $|UT(n, F_q)| = q^{n(n-1)/2}$. 所以 $UT(n, F_q)$ 一定是一个西罗p-子群. ■

推理 6.33 设 p 是一个素数，则每一个有限 p-群 G 均同构于某单位三角群 $UT(m, F_p)$ 的一个子群，其中 $m=|G|$.

证明 我们首先证明，对每一个 $m\geqslant 1$，对称群 S_m 都可以嵌入 $GL(m, k)$ 中，其中 k 为一个

域．令 V 是 k 上一个 m 维向量空间，v_1，…，v_m 为 V 的一组基．定义一个函数 $\varphi: S_m \to \mathrm{GL}(V)$ 为：$\sigma \mapsto T_\sigma$，其中对所有 i 有 $T_\sigma: v_i \mapsto v_{\sigma(i)}$．易见 φ 是一个单同态．

由凯莱定理，G 可嵌入 S_G 中，因此 G 可嵌入 $\mathrm{GL}(m, \mathbb{F}_p)$ 中，其中 $m=|G|$．因为每一个 p-子群包含于某个西罗 p-群内，所以 G 包含于 $\mathrm{GL}(m, \mathbb{F}_p)$ 的某个西罗 p-子群 P 内．因为所有西罗 p-子群是共轭的，所以存在 $a \in \mathrm{GL}(m, \mathbb{F}_p)$ 使得 $P=a(\mathrm{UT}(m, \mathbb{F}_p))a^{-1}$．因此

$$G \cong aGa^{-1} \leqslant a^{-1}Pa \leqslant \mathrm{UT}(m,\mathbb{F}_p). \quad ■$$

一个自然的问题是：求出对称群的所有西罗子群．这个问题可以解决，其解答是用叫做圈积的构造来表示的．

在二十世纪底，经过令人惊奇的集体的努力，所有有限单群被分类了．我们引用高伦斯坦(D. Gorenstein)、利宏斯(R. Lyons)、索罗门(R. Solomon)所著的《有限单群的分类》中下面这段话．

> 有限单群分类的存在性证明散落在有关杂志的 10000 到 15000 页中，分布于超过 100 名数学家的大约 500 篇独立的文章中，这些文章大多数写于 20 世纪 50 年代与 80 年代初期．直到 20 世纪 70 年代攻克完全分类问题的全局策略才被提出．另外，在整个时期新的单群不断被发现，……，所以用精确的方式来表述整个定理是不可能的……这种情况一直持续到 20 世纪 80 年代初期．……考虑到有限单群定理的意义，我们相信，事情的现在这个状态迫使人们去寻找一个更简单的，更加紧凑的和更可及的，且具有更加清楚的基础的证明．……我们给出的论段……大约有 3000 至 4000 页．

现在有一个有限单群的表，它们中的每一个许多重要性质人们已经知道了．许多关于任意有限群的问题可以化归为单群的问题．因此，运用分类定理，只要一个一个地检查，看看表中每一单群是否满足所希望的结果即可． 498

群论的另一个重要的部分是表示论——群至非退化的矩阵群的同态的系统的研究．此理论的第一个应用是伯恩赛德的一个定理：阶为 $p^m q^n$ 的群一定是可解的，其中 p 和 q 是素数．

习题

H 6.20 判断对错并给出理由．

(i)若 G 是一个有限群，p 是一个素数，则 G 只有一个西罗 p-子群．

(ii)若 G 是一个有限阿贝尔群，p 是一个素数，则 G 只有一个西罗 p-子群．

(iii)若 G 是一个有限群，p 是一个素数，则 G 至少有一个西罗 p-子群．

(iv)若 G 作用于一个集 X 上，若 x，$y \in X$ 属于同一个轨道，则 G_x 和 G_y 是 G 的共轭子群．

(v)若 $H \leqslant G$，则 $N_G(H) \lhd G$．

(vi)若 $H \leqslant G$，则 $H \lhd N_G(H)$．

(vii)群 G 的一个西罗 p-子群包含了 G 的所有其他 p-子群．

(viii)若 G 和 H 是同阶的有限群，则对每一个素数 p，它们的西罗 p-子群都是同阶的．

(ix)存在一个 400 阶的群 G，它恰好有 8 个西罗 5-子群．

(x)对 $\mathbb{F}_7$ 上的每一个 10×10 的单位上三角矩阵 B，存在 $\mathbb{F}_7$ 上的一个 10×10 的单位上三角矩阵 A 使得 $AB=BA$．

*6.21 证明 S_4 的西罗 2-子群个数多于 1．

*H 6.22 试给出一个有 3 个西罗 p-子群(对某素数 p)P，Q 和 R 的有限群 G，并且 $P\cap Q=\{1\}$，$P\cap R\neq\{1\}$.

6.23 试证每一个有限 p-群都是可解的.

*H 6.24 **(弗拉蒂尼论断)**令 K 是有限群 G 的一个正规子群. 若 P 是 K 的一个西罗 p-子群，对某素数 p，试证

$$G=KN_G(P),$$

其中 $KN_G(P)=\{ab: a\in K, b\in N_G(P)\}$.

H 6.25 若 F 是具有四个元素的域，试证随机群 $\sum(2, F)\cong A_4$.

H 6.26 试证 S_6 的西罗 2-子群同构于 $D_8\times \mathbb{I}_2$.

H 6.27 令 R 是有限群 G 的一个正规 p-子群，试证对 G 的每个西罗 p-子群 P 均有 $Q\leqslant P$.

499 H 6.28 对有限群 G 的每个素数因子，取定一个西罗 p-子群 Q_p. 试证 $G=\left\langle \bigcup_p Q_p \right\rangle$.

6.29 H (i)设 G 是一个有限群，P 是 G 的一个西罗 p-子群. 若 $H\lhd G$，试证 HP/H 是 G/H 的一个西罗 p-子群且 $H\cap P$ 是 H 的一个西罗 p-子群.

H (ii)设 P 是有限群 G 的一个西罗 p-子群，H 是 G 的一个子群. 试举例 G 与 H 使得 $H\cap P$ 不是 H 的一个西罗 p-子群.

6.30 试证 A_5 的一个西罗 2-子群恰好有 5 个共轭.

H 6.31 试证不存在阶为 300，312，616 或 1000 的单群.

H 6.32 试证若有限群 G 的每一个西罗子群都是正规的，则 G 是它的西罗子群的直积.

6.33 对任一个群 G，试证若 $H\lhd G$，则 $Z(H)\lhd G$.

*H 6.34 若 p 是一个素数，试证每一个 $2p$ 阶的群或者是循环的或者同构于 D_{2p}.

6.35 若 $0\leqslant r\leqslant n$，定义**二项式系数** $\begin{bmatrix} n\\ r\end{bmatrix}_q$ 为$(\mathbf{F}_q)^n$ 中线性无关的 r-表的个数.

H (i)试证

$$\begin{bmatrix} n\\ r\end{bmatrix}_q\begin{bmatrix} n\\ n-r\end{bmatrix}_q=\begin{bmatrix} n\\ n\end{bmatrix}_q$$

(这些系数在超几何系列的研究中出现.)

H (ii)试证在$(\mathbf{F}_q)^n$ 中存在 $\begin{bmatrix} n\\ n-r\end{bmatrix}_q$ 个 r-维子空间.

(iii)试证

$$\begin{bmatrix} n\\ r\end{bmatrix}_q=\frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)(q^{n-r-1})(q^{n-r}-1)\cdots(q-1)}.$$

(iv)试证下类似于引理 1.17 的结论:

$$\begin{bmatrix} n\\ r\end{bmatrix}_q=\begin{bmatrix} n-1\\ r-1\end{bmatrix}_q+q^r\begin{bmatrix} n-1\\ r\end{bmatrix}_q.$$

(v)试证下类似于习题 1.34 的结论:

$$\begin{bmatrix} n\\ r\end{bmatrix}_q=\frac{q^n-1}{q^r-1}\begin{bmatrix} n-1\\ r-1\end{bmatrix}_q.$$

6.36 求 $Z(UT(3, \mathbf{F}_q))$和 $Z(UT(4, \mathbf{F}_q))$.

6.37 (i)试证 $UT(n, \mathbf{F}_q)$有正规系列

$$UT(n,\mathbf{F}_q)=G_0\geqslant G_1\geqslant\cdots\geqslant G_n=\{1\}$$

其中 $G_i \cong \mathrm{UT}(i, \mathbb{F}_q)$，$G_i$ 由所有主对角线上方的 i 个斜对角线上的元素均为零的 $n\times n$ 单位三角矩阵组成. 例如，G_1 由所有具有形式 $\begin{bmatrix}1&0&*&*&*\\0&1&0&*&*\\0&0&1&0&*\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$ 的矩阵组成，而 G_2 由所有具有形式 $\begin{bmatrix}1&0&0&*&*\\0&1&0&0&*\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$ 的矩阵组成.

(ii)试证商群 G_{i-1}/G_i 是交换的，对所有的 $i\geqslant 1$.

6.38 **H** (i)试证 $|\mathrm{GL}(n, \mathbb{F}_q)| = (q-1)|\mathrm{SL}(n, \mathbb{F}_q)|$.

H (ii)试证 $|\mathrm{SL}(2, \mathbb{F}_5)| = 120$.

H (iii)求 $\mathrm{SL}(2, \mathbb{F}_5)$的一个西罗 2-子群. 500

6.3 装饰的对称

在 2.3 节中，我们称平面的等距同构为保持距离不变的函数 $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$. 在命题 2.61 中，我们说平面的所有等距同构构成的集合 $\mathbf{Isom}(\mathbb{R}^2)$关于合成是一个群. 对平面的任一个子集 Ω，它的对称群定义为

$$\Sigma(\Omega) = \{\varphi \in \mathbf{Isom}(\mathbb{R}^2) : \varphi(\Omega) = \Omega\}.$$

例如，我们在定理 2.65 中看到，二面体群 D_{2n}同构于一个正 n-边形 Ω 的对称群. 在本节中，我们将研究特定的设计(称之为"楣")的对称群，我们的讨论是仿照伯恩(Burn)的《群：通向几何之路》(Groups: A Path to Geometry)中的内容进行的.

在例 2.57 中，我们定义了三种等距同构：旋转、反射和平移(存在第四种，见定理 6.42). 通过$(a, b)\mapsto a+\mathrm{i}b$，将平面$\mathbb{R}^2$ 与复数$\mathbb{C}$ 等同起来. 因此，每个点$(x, 0)$与实数 x 等同(特别地，原点与 0 等同)，x-轴与$\mathbb{R}$ 等同. 用记号 $\mathrm{e}^{\mathrm{i}\theta}$而不是正常的记号 $\mathrm{e}^{2\pi\mathrm{i}\theta}$表示在单位圆上的数. $\mathbb{R}^2$ 与$\mathbb{C}$ 的等同使得我们可以给出等距同构的简单的代数公式. 请将下列与例 2.57 中的几何描述作比较.

例 6.34 (i)关于原点转 θ 角度的**旋转**是将极坐标为(r, α)的点变成极坐标为$(r, \theta+\alpha)$的点的函数 R_θ，此等距同构可写成 $R_\theta: z\mapsto \mathrm{e}^{\mathrm{i}\theta}z$，因为若 $z=r\mathrm{e}^{\mathrm{i}\alpha}$，则

$$R_\theta(z) = \mathrm{e}^{\mathrm{i}\theta}z = \mathrm{e}^{\mathrm{i}\theta}r\mathrm{e}^{\mathrm{i}\alpha} = r\mathrm{e}^{\mathrm{i}(\theta+\alpha)}.$$

(ii)一个等距同构 ρ_ℓ 为一个**反射**，若存在一条直线 ℓ，称为**轴**，其上的每一点都被 ρ_ℓ 固定，并且此直线垂直等分所有端点为 z，$\rho_\ell(z)$的线段. 特别地，关于 x-轴的反射将点(a, b)变成$(a, -b)$，这就是复共轭 $\sigma: z=a+\mathrm{i}b\mapsto a-\mathrm{i}b=\bar{z}$.

(iii)沿向量 c 的**平移**为$\tau_c: z\mapsto z+c$. 记住，恒等变换 $z\mapsto z$ 是一个平移，它是唯一的具有一个固定点的平移. ◀

回忆一下，若 φ 是一个等距同构，则当 ℓ 为一条直线时，$\varphi(\ell)$也是一条直线，且当 C 为一

个圆时，$\varphi(C)$也是一个圆．更详细地，若 $\ell=L[P, Q]$是由不同的点 P 和 Q 确定的直线，则由引理 2.58 有 $\varphi(L[P, Q])=L[\varphi(P), \varphi(Q)]$．若 $C=C[P; PQ]$是圆心为 P 半径为 PQ 的圆，则$\varphi(C[P; PQ])=C[\varphi(P); \varphi(P)\varphi(Q)]$．

501 下面是一条几何的引理．

引理 6.35 设 A，P，Q 为平面中的不同的点，$C=C[P; PA]$是圆心为 P 半径为 PA 的圆，$C'=C[Q; QA]$是圆心为 Q 半径为 QA 的圆，则 $C\cap C'=\{A\}$ 当且仅当 A，P，Q 是共线的．

证明 我们应用解析几何的方法．作 P 和 Q 为 x-轴上的点$(0, 0)$和点$(1, 0)$，设 $A=(a, b)$，则 C 的方程为 $x^2+y^2=|PA|^2=a^2+b^2$，C'的方程为$(x-1)^2+y^2=|QA|^2=(a-1)^2+b^2$．若 $B=(p, q)\in C\cap C'$，则有方程

$$p^2+q^2=a^2+b^2 \quad 和 \quad (p-1)^2+q^2=(a-1)^2+b^2.$$

因此，

$$(p-1)^2+(a^2+b^2-p^2)=(a-1)^2+b^2.$$

化简后即得 $p=a$ 和 $q=\pm b$．若 $b\neq 0$，则 $C\cap C'$中就有两点．因此，若 $C\cap C'$中仅有一点，则 $b=0$．但此点一定为 A，故 $A=(a, 0)$．从而 A 点落在 x-轴上，即 A，0 和 1 是共线的．反之，若 $C\cap C'$中的点多于一个，则 $C\cap C'=\{A, B\}\neq\{A\}$．因此 $B=(a, -b)\neq(a, b)=A$，从而 $b\neq 0$，故 A，P，Q 是不共线的． ■

命题 6.36 设 $\varphi: \mathbb{C}\to\mathbb{C}$ 是一个固定 0 的等距同构．

(i)存在满足 $\varphi(1)=e^{i\theta}$的某 θ．若 $\varphi(1)=1$，则 φ 固定 x-轴上的每一点且 φ 为一个恒等变换或复共轭．

(ii)若 $\varphi(1)\neq 1$，则 φ 为一个旋转或反射．更详细地，当 φ 为一个旋转时，$\varphi: z\mapsto e^{i\theta}z$；当 φ 为一个反射时，$\varphi: z\mapsto e^{i\theta}\bar{z}$．在后一种情形，$\varphi$ 的反射轴是 $\ell=\{re^{i\theta/2}: r\in\mathbb{R}\}$．在两种情形中，$\varphi$ 都是落在正交群 $O_2(\mathbb{R})$ 中的一个线性变换．

证明 (i)设 $z\in\mathbb{R}$ 不是 0，$C_{|z|}$ 是圆心为 0 半径为 $|z|=|0z|$ 的圆．因为 φ 是一个固定 0 的等距同构，等距同构将一个圆变成另一个同样半径的圆：$\varphi(C[0; 0z])=C[\varphi(0); \varphi(0)\varphi(z)]=C[0; 0\varphi(z)]$，所以我们有 $\varphi(C_{|z|})=C_{|z|}$．特别地，$1\in C_1$ 推出 $\varphi(1)\in C_1$，故对某 θ，$\varphi(1)=e^{i\theta}$．

假设 φ 也固定 1，$z\in\mathbb{R}$ 不为 0，1．若 $C=C[0, z]$，$C'=C[1, z]$，则因为 $|0z|=|\varphi(0)\varphi(z)|=|0\varphi(z)|$，所以 $\varphi(C)=\varphi(C[0, z])=C[0, \varphi(z)]=C$．类似地，$\varphi(C')=C'$．因为 0，1，$z$ 是共线的，故由引理 6.35，$\{z\}=C\cap C'$．因此

$$\{\varphi(z)\}=\varphi(C\cap C')=\varphi(C)\cap\varphi(C')=C\cap C'=\{z\}.$$

502 从而 φ 固定$\mathbb{R}$ 中的每一点．

若 $z\notin\mathbb{R}$，设 C 是圆心为 0 半径为 $0z$ 的圆，C'是圆心为 1 半径为 $1z$ 的圆．注意 $\varphi(C\cap C')=\varphi(C)\cap\varphi(C')=C\cap C'$，由引理 6.35，$C\cap C'=\{z, \bar{z}\}$．故有 $\varphi(z)=z$ 或 $\varphi(z)=\bar{z}$．若对某 $z\notin\mathbb{R}$，$\varphi(z)=z$，则 φ 固定向量空间$\mathbb{R}^2$ 的一组基 1，z，因此 φ 是一个恒等变换(因为由命题 2.59知 φ 是一个线性变换)，从而，若 φ 不是一个恒等变换，则对所有的 z，$\varphi(z)=\bar{z}$．

(ii)设 ψ 为关于 0 点转 θ 角度的旋转，则 $\psi^{-1}\varphi$ 就是一个固定 0 和 1 的等距同构. 由(i)有 $\psi^{-1}\varphi$ 是恒等变换或复共轭. 也就是 $\varphi(z)=e^{i\theta}z$ 或 $\varphi(z)=e^{i\theta}\bar{z}$.

若 $\varphi(z)=e^{i\theta}z$，则例 6.34(i)表明 φ 是一个旋转.

若 $\varphi: z\mapsto e^{i\theta}\bar{z}$，则

$$\varphi(re^{i\theta/2}) = e^{i\theta}\overline{\varphi(re^{i\theta/2})} = re^{i\theta}e^{-i\theta/2} = re^{i\theta/2},$$

故 ℓ 上的每个点都被 φ 固定. 若 $z=re^{i\alpha}\notin\ell$，则 $\varphi(z)=re^{i(\theta-\alpha)}$. 在图 6-1 中，直线 $L=L[z,\varphi(z)]$ 与 ℓ 的交点记为 A，L 与 x-轴的交点记为 U. 我们来证明 ℓ 等分 $\angle z0\varphi(z)$. 又 $\angle U0\varphi(z)=\theta-\alpha$，故 $\angle z0\varphi(z)=\theta-2\alpha=2\left(\frac{1}{2}\theta-\alpha\right)$. 因此 $\angle\varphi(z)0A=\frac{1}{2}\theta-\alpha=\angle z0A$. 因此 $\triangle z0A$ 相似于 $\triangle\varphi(z)0A$. 因为 $|0\varphi(z)|=r=|0z|$，所以 $|\varphi(z)A|=|Az|$. 最后，ℓ 垂直于 $L=L[\varphi(z),z]$，因为 $\angle 0A\varphi(z)=\angle 0Az$ 且它们的和是 180°，所以 φ 关于轴 ℓ 的一个反射. ■

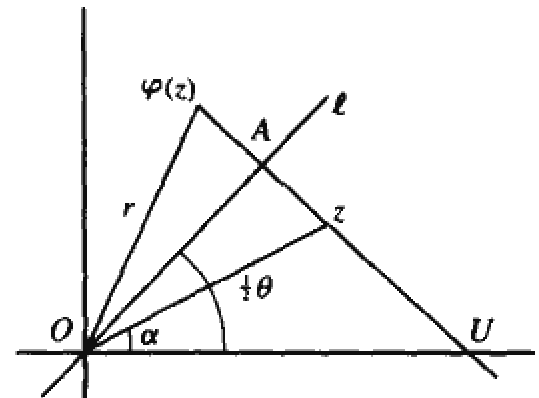


图 6-1 $z\mapsto e^{i\theta}\bar{z}$ 是一个反射

将固定 0 的所有等距同构分类完之后，我们现在来研究任意的等距同构.

推论 6.37 若 φ 是一个满足 $\varphi(0)=c$ 的等距同构，则存在某 θ 使得

$$\varphi(z) = e^{i\theta}z + c \text{ 或 } \varphi(z) = e^{i\theta}\bar{z} + c.$$

证明 若 φ 是一个平移，不妨设 $\varphi: z\mapsto z+c$，则 φ 已具有形式 $\varphi(z)=e^{i\theta}z+c$，其中 $\theta=0$. 一般地，给定 $\varphi: z\mapsto e^{i\theta}z+c$，定义 τ 是移动幅度为 $c=\varphi(0)$ 的平移. 注意 $\tau^{-1}\varphi$ 是一个固定 0 的等距同构，因此由命题 6.36，它是一个旋转或反射. ■ 503

易见等距同构 $z\mapsto e^{i\theta}+c$ 是关于 c 点转 θ 角度的旋转. 第一个猜测是形如 $z\mapsto e^{i\theta}\bar{z}+c$ 的等距同构都是反射，但下述命题表明，这不总是对的.

一个非零复数 $z=re^{i\theta}$ 的**方位**定义为 θ. 每一条直线 ℓ 的方程具有形式 $z=re^{i\theta}+v_0$，其中 $r\in\mathbb{R}$ 且 $v_0\in\mathbb{C}$，我们说 ℓ 的**方位**为 θ.

命题 6.38 下列关于方程 $\varphi: z\mapsto e^{i\theta}\bar{z}+c$ 的等距同构的陈述是等价的.

(i) $\varphi^2=$ 恒等变换.

(ii) $e^{i\theta}\bar{c}+c=0$.

(iii) φ 有一个固定点.

(iv) φ 有一条由固定点构成的直线 ℓ 且 ℓ 的方位是 $\theta/2$.

(v) φ 是一个反射.

证明 (i)⇒(ii).

$$\begin{aligned}\varphi^2(z) &= \varphi(e^{i\theta}\bar{z}+c)\\ &= e^{i\theta}\overline{(e^{i\theta}\bar{z}+c)}+c\\ &= e^{i\theta}(e^{-i\theta}z+\bar{c})+c\\ &= z+e^{i\theta}\bar{c}+c\end{aligned}$$

因此，φ^2 是恒等变换当且仅当 $e^{i\theta}\bar{c}+c=0$.

(ii)⇒(iii). 因为 φ 是一个反射，所以端点为 z 和 $\varphi(z)$ 的线段的中点 $\frac{1}{2}(z+\varphi(z))$ 落于 φ 轴上，因此它被 φ 固定. 特别地，点 $\frac{1}{2}c$ 是被 φ 固定的（它是 0 和 $\varphi(0)=c$ 的中点）. 事实上，$\varphi\left(\frac{1}{2}c\right)=e^{i\theta}\frac{1}{2}\bar{c}+c=\frac{1}{2}(e^{i\theta}\bar{c}+c)+\frac{1}{2}c=\frac{1}{2}c$，因为 $e^{i\theta}\bar{c}+c=0$.

(iii)⇒(iv). 假设 $\varphi(u)=u$. 设直线 $\ell=\{u+re^{i\theta/2}: r\in\mathbb{R}\}$. 显然 ℓ 的方位为 $\theta/2$. 若 $z\in\ell$，则

504

$$\begin{aligned}\varphi(z)&=\varphi(u+re^{i\theta/2})\\&=e^{i\theta}(\overline{u+re^{i\theta/2}})+c\\&=e^{i\theta}\bar{u}+re^{i\theta}e^{-i\theta/2}+c\\&=(e^{i\theta}\bar{u}+c)+re^{i\theta/2}\\&=\varphi(u)+re^{i\theta/2}\\&=u+re^{i\theta/2}\\&=z.\end{aligned}$$

(iv)⇒(v). 只需证明 φ 是轴为 ℓ 的一个反射. 因为 φ 固定 ℓ 上的每一个点，故只需证明，对每一个 $z\notin\ell$，ℓ 垂直等分端点为 z 和 $\varphi(z)$ 的线段. 若 $\psi: z\mapsto e^{i\theta}\bar{z}$，则我们看到在命题 6.36 中，$\psi$ 是轴为 $\ell'=\{re^{i\theta/2}: r\in\mathbb{R}\}$ 的反射. 因此 ℓ' 垂直等分每一条端点为 $z-\frac{1}{2}c$，$\psi\left(z-\frac{1}{2}c\right)$ 的线段. 若定义 τ 为移动幅度为 $\frac{1}{2}c$ 的平移，则 $\ell=\tau(\ell')$ 垂直等分端点为 $\tau\left(z-\frac{1}{2}c\right)$，$\tau\left(\psi(z-\frac{1}{2}c)\right)$ 的线段. 但是 $\tau\left(z-\frac{1}{2}c\right)=z$ 且

$$\begin{aligned}\tau\left(\psi\left(z-\frac{1}{2}c\right)\right)&=e^{i\theta}\left(\overline{z-\frac{1}{2}c}\right)+\frac{1}{2}c\\&=e^{i\theta}\bar{z}-\frac{1}{2}e^{i\theta}\bar{c}+\frac{1}{2}c\\&=[e^{i\theta}\bar{z}+c]-c-\frac{1}{2}e^{i\theta}\bar{c}+\frac{1}{2}c\\&=\varphi(z)-\frac{1}{2}(e^{i\theta}\bar{c}+c)\\&=\varphi(z).\end{aligned}$$

(v)⇒(i). 反射的平方是恒等变换. ■

例 6.39 我们观察到反射和平移是不可交换的. 设 $\sigma: z\mapsto\bar{z}$ 为复共轭，$\tau: z\mapsto z+i$ 是移动幅度为向量 i 的平移. 这样 $\sigma\tau(z)=\overline{z+i}=\bar{z}-i$，而 $\tau\sigma(z)=\bar{z}+i$. ◀

我们现在分析那些不是反射的等距同构 $\varphi: z\mapsto e^{i\theta}\bar{z}+c$.

命题 6.40 若 $\varphi: z\mapsto e^{i\theta}\bar{z}+c$ 不是一个反射，则 $\varphi=\tau\rho$，其中 ρ 是一个反射，不妨设其轴为 ℓ，τ 是一个平移 $z\mapsto z+\frac{1}{2}w$，其中 w 具有与 ℓ 一样的方位.

证明　像在命题 6.38(i)⇒(ii)的证明中一样，我们有 $\varphi^2(z)=z+e^{i\theta}\bar{c}+c$. 我们定义 $w=e^{i\theta}\bar{c}+c$，所以有

$$\varphi^2: z\mapsto z+w. \tag{1}$$

又定义

$$\tau: z\mapsto z+\frac{1}{2}w,$$

则 $\tau^2=\varphi^2$.　505

首先注意到，

$$e^{i\theta}\bar{w}=e^{i\theta}(e^{-i\theta}c+\bar{c})=w. \tag{2}$$

由此得出 w 的方位为 $\frac{1}{2}\theta$：若 $w=re^{i\alpha}$，则在(2)中作替换 $w=e^{i\theta}\bar{w}$ 立即有 $re^{i\alpha}=re^{i\theta}e^{-i\alpha}$. 因此 $e^{2i\alpha}=e^{i\theta}$，故 $\alpha=\frac{1}{2}\theta$.

我们断言 τ 与 φ 可交换.

$$\begin{aligned}\varphi(\tau(z))&=\varphi\left(z+\frac{1}{2}w\right)\\&=e^{i\theta}\overline{\left(z+\frac{1}{2}w\right)}+c\\&=e^{i\theta}\bar{z}+c+\frac{1}{2}e^{i\theta}\bar{w}\\&=\varphi(z)+\frac{1}{2}w\\&=\tau(\varphi(z)).\end{aligned}$$

由此得出 φ 与 τ^{-1} 可交换：

$$\varphi\tau^{-1}=\tau^{-1}(\tau\varphi)\tau^{-1}=\tau^{-1}(\varphi\tau)\tau^{-1}=\tau^{-1}\varphi.$$

但 $\tau^2=\varphi^2$，故

$$(\tau^{-1}\varphi)^2=(\tau^{-1})^2\varphi^2=\text{恒等变换}.$$

因此，若我们定义 $\rho=\tau^{-1}\varphi$，则 $\rho^2=$恒等变换，且

$$\rho(z)=\tau\varphi(z)=e^{i\theta}\bar{z}+\left(c+\frac{1}{2}w\right).$$

由命题 6.38，ρ 是一个轴具有方位 $\frac{1}{2}\theta$ 的反射，而我们已经观察到 w 的方位也为 $\frac{1}{2}\theta$. ■

定义　一个对称 φ 称为是一个**滑动反射**，若 $\varphi=\tau_v\rho$，其中 ρ 是一个轴为 ℓ 的反射，τ_v 是一个平移且 v 具有与 ℓ 相同的方位. 因此，对某非零 $r\in\mathbb{R}$，

$$\varphi(z)=e^{i\theta}\bar{z}+v=e^{i\theta}\bar{z}+re^{i\theta/2}.$$

滑动反射就是命题 6.40 中的等距同构. 请注意，滑动反射 φ 并不是反射，因为 φ^2 不是恒等变换.

例 6.41　等距同构 $\varphi: z\mapsto\bar{z}+1$ 是一个将 x-轴变成自身的滑动反射：$\varphi(\mathbb{R})=\mathbb{R}$. 若△是

顶点为(0, 0), $\left(\frac{1}{2}, 0\right)$, (1, 1)的三角形，则 $\varphi(\triangle)$是顶点为(1, 0), $\left(\frac{3}{2}, 0\right)$, (2, −1)的三角形，$\varphi^2(\triangle)$的顶点为(2, 0), $\left(\frac{5}{2}, 0\right)$, (3, 1)且 $\varphi^n(\triangle)$的顶点为$(n, 0)$, $\left(\frac{2n+1}{2}, 0\right)$, $(n+1, (-1)^n)$. 图 6-2 中的设计可向左和向右无限延长，它在 φ 下是不变的.

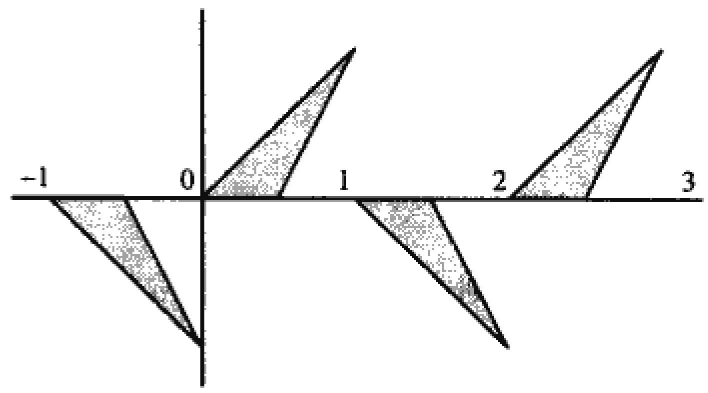


图 6-2 滑动反射

◀

506 下述结论总结了到目前为止我们的工作.

定理 6.42 *每个等距同构或者是平移、旋转、反射，或者是滑动反射.*

证明 由命题 6.36(ii)、6.38 和 6.40 及推论 6.37 可得. ■

推论 6.43 设 $\varphi\in \mathbf{Isom}(\mathbb{R}^2)$.

(i)若 φ 无固定点，则 φ 或者是一个平移或者是一个滑动反射.

(ii)若 φ 仅有一个固定点，则 φ 是一个旋转.

(iii)若 φ 有多于一个固定点，则 φ 或者是一个滑动反射或者是一个恒等变换.

证明 由定理 6.42，仅有四种形式的等距同构：平移，它无固定点；旋转，它只有一个固定点；反射，它有无限多个固定点，也就是它的轴上的每一个点；滑动反射. 只须证明滑动反射 φ 无固定点. 若 $\varphi(z)=z$，则 $\varphi^2(z)=z$，但由(1)有 $\varphi^2=\tau$，其中 $\tau\neq$恒等变换是一个平移，这与平移无固定点的事实相违. ■

例 6.44 我们用定理 6.42 来确定 $\mathbf{Isom}(\mathbb{R}^2)$中的有限阶的元素，(不是恒等变换的)平移是无限阶的，滑动反射也是无限阶的(因为滑动反射的平方是一个平移)，所有反射的阶为 2. 最后，假设 $\varphi: z\mapsto e^{i\theta}z+c$ 是一个(关于 c 点)的旋转. 由归纳法，我们看到

$$\varphi^n(z) = e^{n i\theta}z + c(1 + e^{i\theta} + e^{2i\theta} + \cdots + e^{(n-1)i\theta}).$$

若 $\varphi^n=$恒等映射，则 $\theta=2\pi/n$ 且 $\varphi^n(z)=z+c(1+e^{i\theta}+e^{2i\theta}+\cdots+e^{(n-1)i\theta})$. 注意 $e^{i\theta}$是一个 n 次的
507 单位根，故 $1+e^{i\theta}+e^{2i\theta}+\cdots+e^{(n-1)i\theta}=0$. 从而，若 φ^n 是恒等变换，则我们必有 $c=0$. 也就是，$\varphi(z)=e^{2\pi i/n}z$. 反之，若 $\theta=2\pi/n$，则 $z\mapsto e^{i\theta}z$ 是有限阶的.

除反射之外，还存在阶为 2 的元素吗？这样的等距同构 φ 一定具有形式 $z\mapsto e^{\pi i}z+c$，也就是 $\varphi(z)=-z+c$，称之为**半翻转**. 注意半翻转不是一个反射，因为反射有无限多个固定点，而半翻转作为一个旋转，仅有一个固定点. 一个半翻转将一条直线的方位变号. 例，$\varphi: z\mapsto -z+2$ 将

$$\cdots]-->--]-->--]-->--]-->--]\cdots$$

变成

$$\cdots < - - [- - < - - [- - < - - [- - < - - [- - < \cdots$$

读者可以验证，一个半翻转将一个图形上下颠倒. 例如，$\varphi(\vee)=\wedge$ 且 $\varphi(\wedge)=\vee$. ◀

回忆到，设 z_1，…，z_n 是C中的不同的点，则它们的重心为 u，其中

$$u=\frac{1}{n}(z_1+\cdots+z_n).$$

引理 6.45 *设 $\varphi\in \mathbf{Isom}(\mathbb{R}^2)$，设 z_1，…，z_n 是$\mathbb{R}^2$ 中的不同的点，则 $\varphi(u)=u'$，其中 u 是 z_1，…，z_n 的重心，且 u' 是 $\varphi(z_1)$，…，$\varphi(z_n)$的重心.*

证明 由定理 6.42，φ 是平移，旋转，反射和滑动反射之一. 关于 c 点的旋转是一个复合函数 $\tau\rho$，其中 τ 是平移 $z\mapsto z+c$，ρ 是关于 0 的旋转. 命题 6.40 表明一个滑动反射也是一个平移和一个反射的复合，而每个反射是一个平移和一个轴通过 0 的反射的复合. 因此我们只须证明当 φ 为一个平移或一个关于原点的旋转或轴通过原点的一个反射时(因此在任一情形下，都能确定 0)，$\varphi(u)=u'$.

假设 φ 是一个平移：$\varphi(z)=z+a$. 则

$$\begin{aligned}\varphi(u)&=u+a\\&=\frac{1}{n}(z_1+\cdots+z_n)+a\\&=\frac{1}{n}z_1+\cdots+\frac{1}{n}z_n+\frac{1}{n}a+\cdots+\frac{1}{n}a\\&=\frac{1}{n}(z_1+a)+\cdots+\frac{1}{n}(z_n+a)\\&=\frac{1}{n}\varphi(z_1)+\cdots+\frac{1}{n}\varphi(z_n)\\&=u'.\end{aligned}$$

若 φ 为关于原点的一个旋转或轴通过 0 的一个反射，则由命题 6.36 可知，φ 是一个线性变换，因此

$$\varphi(u)=\varphi\left(\frac{1}{n}[z_1+\cdots+z_n]\right)=\frac{1}{n}[\varphi(z_1)+\cdots+\varphi(z_n)]=u'.$$ ■ 508

引理 6.46 *若 $G\leqslant \mathbf{Isom}(\mathbb{R}^2)$是一个有限子群，则存在 $u\in\mathbb{C}$ 使得 $\varphi(u)=u$，对所有 $\varphi\in G$.*

证明 选择 $z\in\mathbb{C}$. 设$\mathcal{O}$为一个轨道：

$$\mathcal{O}=\{\varphi(z):\varphi\in G\}.$$

因为 G 是有限的，所以$\mathcal{O}$也是有限的：$\mathcal{O}=\{z_1, \cdots, z_n\}$，其中 $z_1=z$. G 作用在$\mathcal{O}$上，因为若 $\psi\in G$，则 $\psi(z_j)=\psi\varphi(z_1)\in\mathcal{O}$，因为 $\psi\varphi\in G$. 因此每一个 $\varphi\in G$ 置换$\mathcal{O}$中的元，因为 φ 是一个单射且 $\varphi:\mathcal{O}\to\mathcal{O}$. 因为 $\varphi\in G$ 置换$\mathcal{O}$中的元，因此$\mathcal{O}$的重心 u 等于 $\varphi(\mathcal{O})=\mathcal{O}$的重心. 因此，由引理 6.45，对所有的 $\varphi\in G$ 有 $\varphi(u)=u$. ■

外尔(H. Weyl)在他的书《对称》(Symmetry)中将下定理归功于达·芬奇(Leonardo da Vinci，1452—1519).

定理 6.47(莱昂那多) 若 $G \leqslant \mathbf{Isom}(\mathbb{R}^2)$ 是一个有限群，则或者 $G \cong \mathbb{I}_m$，对某 m，或者 $G \cong D_{2n}$，对某 n.

证明 由引理 6.46，存在 $c \in \mathbb{C}$ 使得 $\varphi(c)=c$，对所有 $\varphi \in G$. 若 $\tau: z \mapsto z-c$，则 $\tau\varphi\tau^{-1}(0)\tau = \tau\varphi(c)=\tau(c)=0$. 因为 $\tau G\tau^{-1} \cong G$，所以我们可假设每一个 $\varphi \in G$ 固定 0. 因此应用命题 6.36：我们可假设 $G \leqslant O_2(\mathbb{R})$，因此每一个 $\varphi \in G$ 是一个线性变换. 更进一步，我们可假设每一个 $\varphi \in G$ 是一个旋转或一个反射.

假设 G 中不含反射，则 G 的元素是旋转 R_{θ_1}，…，R_{θ_m}，由例 6.44，其中 $\theta_j = 2\pi k_j/n_j$. 若 $n=\max_j\{n_j\}$，则 $G \leqslant \langle R_{2\pi/n}\rangle$. 因此作为一个循环群的子群的 G 本身也是循环的.

假设 G 包含一个反射 ρ. 由习题 6.48，我们可以替换 G 为一个同构于 G 且包含了复共轭 σ 的群. G 中所有旋转构成的子集是一个子群，且是 $\mathbf{Isom}(\mathbb{R}^2)$ 的一个不包含反射的有限子群，因此它是循环的，不妨设为 $H=\langle h\rangle$，其中 $h(z)=e^{i\theta}z$ 的阶为 n. 又 $\sigma h\sigma^{-1}=h^{-1}$，因为

$$\sigma h\sigma^{-1}: z \mapsto \bar{z} \mapsto e^{i\theta}\bar{z} \mapsto \overline{e^{i\theta}\bar{z}} = e^{-i\theta}z = h^{-1}(z).$$

因此，$\langle h, \sigma\rangle = H \cup H\sigma$ 是一个同构于 D_{2n} 的一个子群. 我们断言 $\langle h, \sigma\rangle = G$. 若 $r \in G$ 为一个反射，则 $r(z)=e^{i\alpha}\bar{z}=R_\alpha\sigma(z)$. 但因为它是 G 中的一个旋转，所以 $R_\alpha = r\sigma^{-1} \in H$，所以 $r = R_\alpha\sigma \in \langle h, \sigma\rangle$. ■

莱昂那多定理求出了 $O_2(\mathbb{R})$ 的所有有限的且固定一个点的子群. 我们现在来求 $\mathbf{Isom}(\mathbb{R}^2)$ 的固定一条直线而不是一个点的子群，它被称为楣群. 在同构意义下，只有四种这样的子群. 但当我们考虑几何方面因素时，我们将看到它们有七类.

根据《牛津英语词典》(Oxford English Dictionary)，楣(frieze)是“柱子上的像台子的东西，
509 在柱子的楣的上部分与下部分之间”. 幸运地，它进一步说，楣是“充满雕刻的宽饰带”. 注意雕刻是 3 维的，但我们用“楣”这个词是表示任意(2 维)宽带，它上面的一些图案从左到右无限次地重复. 用更准确的语言，我们说平面的一个子集 F 是一个带，若在对称群 $\Sigma(F)$ 中，存在某个固定一条直线 ℓ 的等距同构 φ(非恒等映射)，也就是 $\varphi(\ell)=\ell$(我们不要求 φ 固定 ℓ 上每一点). 称一个带子 F 是一个楣，就是说存在某种“设计”$D \subseteq F$ 使得 $F=\bigcup_{n\in\mathbb{Z}}\tau^n(D)$，对某平移 $\tau \in \Sigma(F)$. 对某楣 F，我们的目标是分类 $\mathbf{Isom}(\mathbb{R}^2)$ 的所有具有形式 $\Sigma(F)$ 的子群.

图 6-3 中的带 F 是一个楣：它是被平移 $\tau: z \to z+1$ 固定，它的被重复的图案是底为闭区间 $\left[0, \frac{1}{2}\right]$ 的三角形 D.

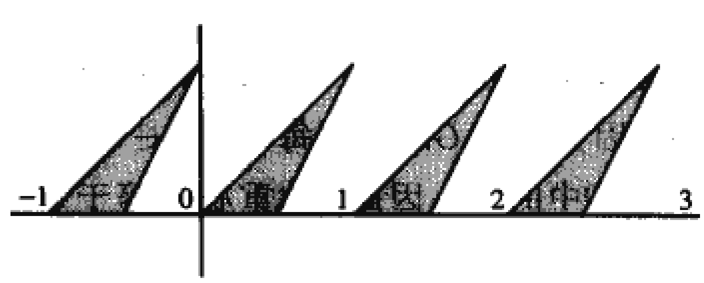


图 6-3　楣 F

考虑在图 6-2 中的带 F'. 易见它的对称群 $\Sigma(F')$ 包含滑动反射 $\varphi: z \mapsto \bar{z}+1$. 注意 $\varphi(\mathbb{R})=\mathbb{R}$ 且 $F'=\bigcup_{n\in\mathbb{Z}}\varphi^n(D)$，其中 D 是底为 $\left[0, \frac{1}{2}\right]$ 的三角形. 这并不表明 F' 是一个楣因为 φ 不是一个平移. 然而，实际上，F' 是一个楣，因为平移 $\tau: z \mapsto z+2$ 在 $\Sigma(F')$ 中且 $F'=\bigcup_{n\in\mathbb{Z}}\tau^n(D')$，其中 D' 是以 $\left[0, \frac{1}{2}\right]$ 为底的三角形和以 $\left[1, \frac{3}{2}\right]$ 为底的三角形的并.



图 6-4　波斯弓箭手

现在考虑楣 F''，它是通过替换图 6-3 中的 F 的以 $\left[0, \frac{1}{2}\right]$ 为底的三角形 D 为另一个图形而得，例如，设 F'' 为图 6-4 中的楣(来自远古苏珊时代的达琳尔宫殿). 图 6-3 中的三角形 D 被替换成一个波斯弓箭手. 显然，$\Sigma(F'')=\Sigma(F)$. 坦白地说，若从几何的角度来分类楣，则存在许多种楣. 例如 D 上应该加什么限制? 尽管如此，如果我们不区分三角形和波斯弓箭手的话，那么我们就有能力对楣进行分类.

记号　$\mathbf{Isom}(\mathbb{R}^2)$ 中的所有平移构成的子群被记为 $\mathbf{Trans}(\mathbb{R}^2)$.

非正式地说，一个楣群就是一个楣的对称群. 我们很快将用一个正式的版本替代下面的定义.

定义 1　一个**楣群**是 $\mathbf{Isom}(\mathbb{R}^2)$ 的一个固定一条直线 ℓ 的子群 G，即对所有 $\varphi\in G$，$\varphi(\ell)=\ell$ 且 $G\cap\mathbf{Trans}(\mathbb{R}^2)$ 是无限循环的. 510

每一个 $\varphi\in G$ 固定一条直线 ℓ 反映如下的事实：一个楣也是一个带. $G\cap\mathbf{Trans}(\mathbb{R}^2)=\langle\tau\rangle$ 是无限循环的则反映下面的事实：一个楣有某重复的设计 $D\subseteq F$，它的 $\langle\tau\rangle$-轨道为 F 的全部.

引理 6.48　若 $\varphi\in G$，其中 G 是一个楣群，则存在某实数 c 使得下列之一成立：

(i) 若 φ 是一个平移，则 $\varphi(z)=z+c$.

(ii) 若 φ 是一个旋转，则 φ 是一个半-翻转：$\varphi(z)=-z+c$.

(iii) 若 φ 是一个反射，则 $\varphi(z)=\bar{z}$ 或 $\varphi(z)=-\bar{z}+c$.

(iv) 若 φ 是一个滑动反射，则 $\varphi: z\mapsto\bar{z}+c$，其中 $c\neq 0$.

证明 我们知道 $\varphi: z\mapsto e^{i\theta}z+c$ 或 $\varphi: z\mapsto e^{i\theta}\bar{z}+c$. 因为 $\varphi(\mathbb{R})=\mathbb{R}$，所以我们有 $c=\varphi(0)\in\mathbb{R}$ 且 $\varphi(1)=e^{i\theta}+c\in\mathbb{R}$. 因此 $e^{i\theta}\in\mathbb{R}$，也就是 $e^{i\theta}=\pm 1$，从而 $\varphi(z)=\pm\bar{z}+c$ 或者 $\varphi(z)=\pm\bar{z}+c$.

剩下的证明就是确定这些公式中的每一个所对应的等距同构的类型. 旋转 θ 角度的旋转公式为 $e^{i\theta}z+c$. 因为 $e^{i\theta}=\pm 1$，所以我们必有 $\theta=\pi$，因此，此时旋转就是半旋转. 等距同构 $\varphi: z\mapsto e^{i\theta}\bar{z}+c$ 是一个反射当且仅当 $e^{i\theta}\bar{c}+c=0$，此时 $\bar{c}=c$，c 是实的，所以 $\bar{c}=c$，因此 φ 是一个反射. 若 $c=0$ 或 $e^{i\theta}=-1$，因此对任意 $c\in\mathbb{R}$，有 $\varphi(z)=\bar{z}$ 或者 $\varphi(z)=-\bar{z}+c$. 最后，若 $c\neq 0$，
511 且 $\varphi(z)=\bar{z}+c$，则 $e^{i\theta}\bar{c}+c=2c\neq 0$ 且 φ 是一个滑动反射. ■

我们打算用两种方式来规范化楣群的分类. 首先，不失一般性，假设被固定的直线 ℓ 是实轴 $\mathbb{R}$，因为我们可以在不改变对称性的情况下，改变坐标轴的位置. 其次，我们将忽略数量上的改变. 例如，图 6-3 中的楣 F 有一个无限循环对称群，也就是 $\sum(F)=\langle\tau\rangle$，其中 τ 是一个平移 $\tau: z\mapsto z+1$. 另一方面，若 $\mathbb{R}^2$ 中的每一个向量在大小上都变成两倍，则 F 变成了一个新的楣 Φ，且 $\sum(\Phi)=\langle\tau'\rangle$，其中 $\tau': z\mapsto z+2$，因此 F 和 Φ 实质上是同一个楣，只是在大小上不同，但它的对称群是不同的因为 $\tau\notin\sum(\Phi)$. 定义以 $\omega: \mathbb{R}^2\to\mathbb{R}^2$ 为 $\omega(z)=2z$. ω 定义了同构 $\sum(F)\to\sum(\Phi): \rho\mapsto w\varphi w^{-1}$. 注意

$$\omega\tau\omega^{-1}: z\mapsto\frac{1}{2}z\mapsto\frac{1}{2}z+1\mapsto 2\left(\frac{1}{2}z+1\right)=z+2.$$

我们第二个规范化的做法是假设 $G\cap\mathbf{Trans}(\mathbb{R}^2)$ 的生成元 τ 是平移 $\tau: z\mapsto z+1$. 由到目前为止的讨论，只须分类规范化的楣群.

定义 2 *一个正规化的楣群是一个子群 $G\leqslant\mathbf{Isom}(\mathbb{R}^2)$，它固定 $\mathbb{R}$ 且 $G\cap\mathbf{Trans}(\mathbb{R}^2)=\langle\tau\rangle$，其中 $\tau: z\mapsto z+1$.*

当我们假设楣群 G 是规范化的时候，引理 6.48 可以被简化. 若 $\gamma: z\mapsto\bar{z}+c$ 是 G 中的一个滑动反射，则 γ^2 也是一个平移，事实上 $\gamma^2: z\mapsto z+2c$. 但 G 中所有的平移在 $\langle\tau\rangle$ 中，所以对某些 $n\in\mathbb{Z}$ 有 $\gamma^2=\tau^n: z\mapsto z+n$. 从而 $2c=n$，所以 $c=m$ 或者对某 $m\in\mathbb{Z}$ 有 $c=m+\frac{1}{2}$. 因此若 $c=m$，G 包含 $\tau^{-m}\gamma=\sigma$，也就是 $\sigma(z)=\bar{z}$，或者若 $c=m+\frac{1}{2}$，$\tau^{-m}\gamma: z\mapsto\bar{z}+\frac{1}{2}$. 为了将 $\gamma\in G$ 与 $\sigma\in G$ 区分开，我们选择 $\gamma: z\mapsto\bar{z}+\frac{1}{2}$ 使得 $\gamma^2=\tau$. 我们也可以规范化半翻转 R 和反射 ρ 使得 $R: z\mapsto -z+1$ 和 $\rho: z\mapsto -\bar{z}+1$.

若 $\varphi\in\mathbf{Isom}(\mathbb{R}^2)$，让我们记 $\varphi(z)=e^{i\theta}z^{\epsilon}+c$，其中 $\epsilon=\pm 1$，$z^1=z$ 且 $z^{-1}=\bar{z}$. 若 $\psi=e^{i\alpha}z^{\eta}+d$，则易见

$$\varphi\psi(z)=e^{i(\theta+\alpha)}z^{\epsilon\eta}+e^{i\theta}d+c.$$

从而有函数 $\pi: \mathbf{Isom}(\mathbb{R}^2)\to O_2(\mathbb{R})$，定义如下

$$\pi: \varphi \mapsto \tau_{\varphi(0)}^{-1} \varphi,$$

它是一个同构[当然，$\tau_{\varphi(0)}^{-1} \varphi: z \mapsto e^{i\theta} z^{\epsilon}$]，且核 $\ker\pi = \mathbf{Trans}(\mathbb{R}^2)$，所以 $\mathbf{Trans}(\mathbb{R}^2) \lhd \mathbf{Isom}(\mathbb{R}^2)$.

定义 设 $\pi: \mathbf{Isom}(\mathbb{R}^2) \to O_2(\mathbb{R})$ 是刚才定义的映射(去掉平移中的常数). 若 G 是一个楣群，则它的**点群**是 $\pi(G)$.

由第二同构定理得出，若 $T = G \cap \mathbf{Trans}(\mathbb{R}^2)$，则 $T \lhd G$ 且 $T \lhd G$ 且 $G/T \cong \pi(G)$. 512

推论 6.49 一个楣群 G 的点群 $\pi(G)$ 是 $\mathrm{im}\pi = \{1, f, g, h\} \leqslant O_2(\mathbb{R})$ 的一个子群(它与四元群 $\mathbf{V}$ 同构)，其中 $f(z) = -z$，$g(z) = -\bar{z}$ 且 $h(z) = \bar{z}$.

证明 由引理 6.48，我们有 $\mathrm{im}\pi = \{1, f, g, h\}$. ∎

我们现在来分类(规范化的)楣群，因为 $\mathrm{im}\pi = \langle f, g, h \rangle$ 同构于四元群，所以它正好有 5 个子群 $\{1\}$，$\langle f \rangle$，$\langle g \rangle$，$\langle h \rangle$ 和 $\langle f, g, h \rangle = \mathrm{im}\pi$，因此存在 5 个点群. 我们来应用习题 2.101. 设 $\pi: G \to H$ 是满足 $\ker\pi = T$ 的一个满同态. 若 $H = \langle X \rangle$，且对每一个 $x \in X$，选择满足 $\pi(g_x) = x$ 的一个提升 $g_x \in G$，则 G 由 $T \cup \{g_x : x \in X\}$ 生成. 而 $T = G \cap \mathbf{Isom}(\mathbb{R}^2) = \langle \tau \rangle$，其中 $\tau: z \mapsto z+1$.

下面这个群会出现在楣群的分类中. 回忆到二面体群 D_{2n} 是由两个元素 a 和 b 生成的一个群，其中 $b^2 = 1$，$a^2 = 1$ 且 $bab = a^{-1}$.

定义 **无限二面体群** D_∞ 是一个由两个元素 a 和 b 生成的一个无限群，其中 $b^2 = 1$ 且 $bab = a^{-1}$.

由习题 6.51，任意两个无限二面体群是同构的.

定理 6.50 至多存在 7 种楣群 G.

证明 我们用表 6-1 中的记号.

表 6-1 正规化的升提

等距	同构公式	类型	升提	阶
τ	$z+1$	平移	1	∞
R	$-z+1$	半-旋转	f	2
ρ	$-\bar{z}+1$	反射	g	2
σ	$\bar{z}$	反射	h	2
γ	$\bar{z}+\frac{1}{2}$	滑动反射	h	∞

情形 1 $\pi(G) = \{1\}$. 在这种情形下，$G = G_1 = \langle \tau \rangle$. 当然 $G_1 \cong \mathbb{Z}$.

情形 2 $\pi(G) = \langle f \rangle$. 此时，$G = G_2 = \langle \tau, R \rangle$. 又 $R^2 = 1$，$R\tau R: z \mapsto z-1$，也就是 $R\tau R = \tau^{-1}$. 因为 G_2 是无限群(因为 τ 的阶是无限的)，所以 G_2 是无限二面体群，也就是 $G_2 \cong D_\infty$.

情形 3 $\pi(G) = \langle g \rangle$. 在此时，$G_3 = \langle \tau, \rho \rangle$. 又 $\rho^2 = 1$ 且 $\rho\tau\rho: z \mapsto z-1$，也就是 $\rho\tau\rho = \tau^{-1}$.

513 因此 $G_3 \cong D_\infty$.

群 G_2 也是无限二面体的，由习题 6.51，所以 $G_3 \cong G_2$，因此 G_2 和 G_3(从代数角度上看)是一样的. 然而这些群在几何上是不同的，因为 G_2 仅包含平移和半翻转，群 G_3 包含一个反射.

情形 4 和情形 5 中，$\pi(G)=\langle h\rangle$. 存在两种可能的情景，因为 h 有两种可能的提升，也就是 σ 和 γ.

情形 4 $G_4=\langle\tau, \sigma\rangle$. 注意 τ 和 σ 是交换的，因为 $\sigma\tau$ 和 $\tau\sigma$ 中每一个均为 $z \mapsto \bar{z}+1$，所以 G_4 是交换的. 进一步，$\sigma^2=1$. 从命题 2.127 易知：

$$G_4 = \langle\sigma\rangle \times \langle\tau\rangle \cong \mathbb{I}_2 \times \mathbf{Z}.$$

情形 5 $G_5=\langle\tau, \gamma\rangle$. 注意 γ 和 τ 交换，因为 $\gamma\tau$ 和 $\tau\gamma$ 中每一个均为 $z \mapsto \bar{z}+\frac{3}{2}$，所以 G_5 是交换的. 因为 $\gamma^2=\tau$，所以 $G_5=\langle\tau, \gamma\rangle=\langle\gamma\rangle$是生成元为 γ 的循环群，也就是 $G_5 \cong \mathbf{Z}$.

G_5 和 G_1 在代数上是一样的，因为它们都是无限循环的，但这些群在几何上是不同的，因为 G_5 含有一个滑动反射而 G_1 只含有平移.

情形 6 和情形 7 中，$\pi(G)=\langle f, g, h\rangle$. 再一次，存在两个可能的情形因为 h 有两个可能的提升. 注意在四元群中，任意两个非单位元的乘积是第三个元素，所以$\langle\tau, R, \sigma\rangle$和$\langle\tau, R, \gamma\rangle$的点群都是$\langle f, g, h\rangle$.

情形 6 $G_6=\langle\tau, R, \sigma\rangle$. 注意同情形 4 中一样，$\sigma\tau=\tau\sigma$. 而 $\sigma R=R\sigma: z \mapsto -\bar{z}+1$. 由此得出$\langle\sigma\rangle \lhd G_6$ 和$\langle\tau, R\rangle \lhd G_6$. 因为$\langle\sigma\rangle \cap \langle\tau, R\rangle=\{1\}$，$G_6$ 是由这两个子群生成，命题 2.127 表明 $G_6=\langle\sigma\rangle \times \langle\tau, R\rangle$. 由情形 2，$\langle\tau, R\rangle \cong D_\infty$，所以且 $G_6 \cong \mathbb{I}_2 \times D_\infty$.

情形 7 $G_7=\langle\tau, R, \gamma\rangle$. 因为 $\gamma^2=\tau$，所以我们有 $G_7=\langle R, \gamma\rangle$. 又 $R^2=1$，$R\gamma R: z \mapsto \bar{z}-\frac{1}{2}$，所以 $R\gamma R=\gamma^{-1}$. 从而 $G_7 \cong D_\infty$.

G_7，G_2 和 G_4 在代数上是一样的，因为每一个都同构于 D_∞. 但这些群在几何上是不同的，因为和均不含有一个滑动反射(以免它们的点群太大). ■

定理 6.51 *7 个可能的楣群每一个都会出现.*

证明 图 6-5 中描述的群中的每一个都有确定的对称构成的群. 我们应该将每一个楣看成被 x-轴二等分，因此每一个字母有一半在 x-轴上方，有一半在下方. 例如，F_4 被 σ 固定，但不被 γ 固定. 为证明这个定理，我们来考虑(规范化的)等距同构 τ，R，ρ，σ 和 γ 中的每一个，且来证明一个给定的楣被它们中的某些固定，其余的不固定.

F_1:	F	F	F	F	F	F	$G_1=\langle\tau\rangle$
F_2:	Z	Z	Z	Z	Z	Z	$G_2=\langle\tau, R\rangle$
F_3:	A	A	A	A	A	A	$G_3=\langle\tau, \rho\rangle$
F_4:	D	D	D	D	D	D	$G_4=\langle\tau, \sigma\rangle$
F_5:	DW	DM	DW	DM	DW	DM	$G_5=\langle\tau, \gamma\rangle$
F_6:	I	I	I	I	I	I	$G_6=\langle\tau, R, \sigma\rangle$
F_7:	MW	MW	MW	MW	MW	MW	$G_7=\langle R, \gamma\rangle$

图 6-5 7 种楣

我们提醒读者注意基本等距同构的几何观点. 平移 τ 是向右移动一个单位，而 σ 是关于 x-轴的一个反射，ρ 是关于 y-轴的反射. 滑动反射 γ 是关于 x-轴的一个反射，接着向右移动半个单位，而半旋转 R 将一个楣上下颠倒. 514

(i)因为 $\sum(F_1)=\langle\tau\rangle$，所以我们有 $\tau(F_1)=F_1$. 但没有一个其他的等距同构固定它，因此 G_1 是一个楣群.

(ii)因为 τ，R 固定 F_2，所以我们有 $\sum(F_2)=\langle\tau, R\rangle$. 但 ρ，σ 和 γ 均不固定它，因此 G_2 是一个楣群.

(iii)因为 τ，ρ 固定 F_2，所以我们有 $\sum(F_3)=\langle\tau, \rho\rangle$. 但 R，σ 和 γ 均不固定它，因此 G_3 是一个楣群.

(iv)因为 τ，σ 固定 F_2，所以我们有 $\sum(F_4)=\langle\tau, \sigma\rangle$. 但 R，ρ 和 γ 均不固定它，因此 G_4 是一个楣群.

(v)因为 τ，γ 固定 F_2，所以我们有 $\sum(F_5)=\langle\tau, \gamma\rangle$. 但 R，ρ 和 σ 均不固定它，因此 G_5 是一个楣群.

(vi)因为所有等距同构都固定 F_6，所以我们有 $\sum(F_6)=\langle\tau, R, \sigma\rangle$. 因此 G_6 是一个楣群.

(vii)因为除 σ 外所有等距同构都固定 F_7，所以我们有 $\sum(F_7)=\langle\tau, R, \gamma\rangle=\langle R, \gamma\rangle$. 因此 G_7 是一个楣群. ■

推理 6.52 *在同构意义下一共存在 4 种楣群，也就是* $\mathbb{Z}$，D_∞，$\mathbb{I}_2\times\mathbb{Z}$ *和* $\mathbb{I}_2\times D_\infty$.

证明 与定理 6.50 中的叙述的一样，$\sum(F_1)$ 和 $\sum(F_5)$ 同构于 $\mathbb{Z}$，$\sum(F_2)$ 和 $\sum(F_3)$ 和 $\sum(F_7)$ 同构于 D_∞，$\sum(F_4)$ 同构于 $\mathbb{I}_2\times\mathbb{Z}$，且 $\sum(F_6)\cong\mathbb{I}_2\times D_\infty$. ■

楣是含有一个轴的平面图形，下一个问题是**墙纸群**的分类，墙纸群是含有两个轴的平面图形的对称群. 设 $B_r(u)=\{v\in\mathbb{R}^2: |v-u|<r\}$ 是圆心为 u 半径为 r 的开圆盘. 当然，子群 $G\leqslant\mathbf{Isom}(\mathbb{R}^2)$ 可作用在 $\mathbb{R}^2$ 上，这样任意点 $u\in\mathbb{R}^2$ 的轨道 $\mathcal{O}(u)$ 有意义：$\mathcal{O}(u)=\{\varphi(u): \varphi\in G\}$. 子群 $G\leqslant\mathbf{Isom}(\mathbb{R}^2)$ 是**离散的**若对每一个 $u\in\mathbb{R}^2$，存在 $r>0$ 使得 $B_r(u)\cap\mathcal{O}(u)=\{u\}$. 可以证明楣群是 $\mathbf{Isom}(\mathbb{R}^2)$ 的那些离散的子群，它固定一条直线而不是一个点(点群固定一个点). **墙纸群**是 $\mathbf{Isom}(\mathbb{R}^2)$ 的那些离散的子群，它不固定一条直线或一个点，若 G 是一个墙纸群，则同态 $\pi: G\to O_2(\mathbb{R})$ 的核为 $\mathbf{Trans}(\mathbb{R}^2)\cap G$，它是一个自由交换群 $\mathbb{Z}\times\mathbb{Z}$. π 的象，仍然称为**点群**，且一定是 $\mathbb{I}_n$ 或 D_{2n} 之一，其中 $n\in\{1, 2, 3, 4, 6\}$(这是所谓的晶体图像限制). 我们推荐有兴趣的读者参阅伯恩的书：《群：通向几何之路》的最后一章，那里证明了恰好存在 17 种墙纸群. 515

在 3-维空间中也存在类似的问题，人们可以分类 5 种柏拉图固体，并给出它们的等距同构群：晶体四面体的对称群为 A_4，三面体和八面体的对称群为 S_4，十二面体和二十面体的对称群为 A_5. **晶体群**定义为离散子群 $G\leqslant\mathbf{Isom}(\mathbb{R}^3)$，它不固定一个点，一条直线或一张平面. 存在一个同态 $G\to O_3(\mathbb{R})$，$\mathbb{R}^3$ 上的所有的正交线性变换. 此同态推广了同态 π，且它的核 $\mathbf{Trans}(\mathbb{R}^3)\cap G$ 是一个自由交换群 $\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}$，它的象，一个点群，是 $O_3(\mathbb{R})$ 的一个有限子群. 存在 230 种晶体群.

习题

H 6.39 判断对错并给出理由.

(i)在平面上存在具有有限个对称群的楣.

(ii)存在恰好有两个固定点的平面的等距同构.

(iii)平面的一个等距同构可以既为一个平移又为一个滑动反射.

(iv)平面的一个等距同构可以既为一个反射又为一个滑动反射.

(v)存在同构于 S_3 的 $\mathbf{Isom}(\mathbb{R}^2)$的一个子群.

(vi)存在同构于 S_4 的 $\mathbf{Isom}(\mathbb{R}^2)$的一个子群.

(vii)两个具有相同的点群的(规范化的)楣群是同构的.

(viii)一个无限二面体群有有限指数的子群.

6.40 (i)若 $\varphi\in\mathbf{Isom}(\mathbb{R}^2)$，则 $\varphi(z)=e^{i\theta}z+c$ 或 $\varphi(z)=e^{i\theta}\overline{z}+c$. 试证 θ 和 c 是被 φ 唯一确定的.

(ii)试证由 $\varphi\mapsto\varphi\tau_{\varphi(0)}^{-1}$ 定义的函数 $f:\mathbf{Isom}(\mathbb{R}^2)\to O_2(\mathbb{R})$是一个同态，其中 $\tau_{\varphi(0)}$ 是平移 $z\mapsto z+\varphi(0)$. 试证同态 f 是满射，它的核是所有平移构成的子群 T. 由此得出结论 $T\lhd\mathbf{Isom}(\mathbb{R}^2)$.

6.41 试证 $\varphi:(x,y)\mapsto(x+2,-y)$是一个等距同构. 它是何类的等距同构?

6.42 检验下列公式.

(i)若 $\tau:z\mapsto z+c$，则 $\tau^{-1}:z\mapsto z-c$.

(ii)若 $R:z\mapsto e^{i\theta}z+c$，则 $R^{-1}:z\mapsto e^{-i\theta}(z-c)$.

516 (iii)若 $\varphi:z\mapsto e^{i\theta}\overline{z}+c$，则 $\varphi^{-1}:z\mapsto e^{i\theta}\overline{(z-c)}$.

(iv)举等距同构 α 和 β 的例子，使得 α 和 $\beta\alpha\beta^{-1}$ 是不同类型的等距同构.

6.43 (i)试证 $\mathbf{Isom}(\mathbb{R}^2)$中的共轭的元素的固定点的数量相同.

(ii)试证若 φ 是一个旋转，ψ 是一个反射，则 φ 和 ψ 在 $\mathbf{Isom}(\mathbb{R}^2)$中是不共轭的.

6.44 若 φ 和 ψ 是 $\mathbf{Isom}(\mathbb{R}^2)$中具有不同的固定点的旋转，试证它们生成的子群$\langle\varphi,\psi\rangle$是无限的.

6.45 若 $\varphi\in\mathbf{Isom}(\mathbb{R}^2)$固定三个非共线的点，试证 φ 是恒等变换.

6.46 (i)试证 $\mathbf{Isom}(\mathbb{R}^2)$中的两个反射的合成或者是一个旋转或者是一个平移.

(ii)试证每一个旋转都是两个反射的合成. 试证每一个平移都是两个反射的合成.

(iii)试证每一个等距同构$\mathbb{R}^2\to\mathbb{R}^2$ 是至多三个反射的合成.

6.47 若 H 表示 $\mathbf{Isom}(\mathbb{R}^2)$的所有固定$\mathbb{R}$ 的等距同构组成的子群，试证复共轭在中心 $Z(H)$中.

*6.48 **H** (i)若 ρ 是 $O_2(\mathbb{R})$中的一个反射，试证存在一个旋转 $R\in O_2(\mathbb{R})$使得 $R\rho R^{-1}=\sigma$，其中 $\sigma(z)=\overline{z}$.

(ii)若 G 是 $O_2(\mathbb{R})$中一个的包含一个反射 ρ 的子群，试证存在一个旋转 $R\in\mathbf{Isom}(\mathbb{R}^2)$使得 RGR^{-1}包含复共轭.

*6.49 试证两个反射的复合或者是恒等变换或者是一个旋转.

*6.50 试证若一个楣群 G 包含下列类型中的等距同构中的两种：半翻转，滑动反射，关于垂直轴的反射，则 G 包含第三种的等距同构.

***H** 6.51 试证任意两个无限二面体群是同构的. 更详细地，设 $G=\langle a,b\rangle$和 $H=\langle c,d\rangle$是两个无限群，且满足 $a^2=1$，$aba=b^{-1}$，$c^2=1$ 和 $cdc=d^{-1}$. 试证 $G\cong H$.

6.52 求下列楣的等距同构群.

(i)SANTACLAUSSANTACLAUSSANTA

(ii) HOHOHOHOHOHOHOHOHOHOHOHO

(iii) ↗↖↗↖↗↖↗↖↗↖↗↖

(iv) ↗ ↗ ↗ ↗ ↗ ↗ ↗
　↘ ↘ ↘ ↘ ↘ ↘ ↘

(v) ↗↖↗↖↗↖↗↖↗↖↗↖
↘↙↘↙↘↙↘↙↘↙↘↙

(vi) ↗↖ ↗↖ ↗↖ ↗↖
↘↙ ↘↙ ↘↙

(vii) ↗↗↗↗↗↗↗↗↗↗↗↗ 517
↘↘↘↘↘↘↘↘↘↘↘↘

第7章 交换环Ⅱ

7.1 素理想和极大理想

在本章中，我们主要研究具有多个变量的多项式. 在解析几何中我们看到，多项式对应于几何图形. 例如，$f(x, y)=x^2/a^2+y^2/b^2-1$ 就与平面 $\mathbb{R}^2$ 上的一个椭圆紧密相联. 在环 $k[x_1, \cdots, x_n]$(k 是一个域)与 k^n 的子集的几何学之间，有比上面更进一步的紧密联系. 给定一组 n 元多项式 $f_1, \cdots, f_t$，称它们共同的根构成的子集 $V\subseteq k^n$ 为一个代数集. 当然，可以研究代数集，因为多项式方程组(线性方程组的明显推广)的解本身是有趣的，而且代数集的出现相当自然. 例如，一个问题的研究经常归结为通过一个代数集来参数化此问题的解，因此理解代数集及它的性质(例如，不可约性、维数、类及奇异性等等)可以使得我们更好地理解原来的问题. $k[x_1, \cdots, x_n]$和代数集之间的相互影响发展成为当今称为代数几何的学科. 本章可以看成此学科的一个介绍.

与通常一样，在讨论多项式环之前，我们先看看更一般的情形(即交换环情形)，这样可能会更简单一些. 我们前面所说的数论中一大部分是与整除性相关的：给定两个整数 a 和 b，$a\mid b$何时成立？即何时有 b 为 a 的倍数？此问题可以转化为关于主理想的问题，因为 $a\mid b$ 当且仅当$(b)\subseteq(a)$. 我们从给出类似于定理 2.123(群的对应定理)的结论的证明开始. 回忆到若 $f: X\to Y$ 是一个函数且 $B\subseteq Y$ 是一个子集，则它的逆象为

518 $$f^{-1}(B)=\{x\in X: f(x)\in B\}.$$

命题 7.1(环的对应定理) 若 I 是交换环 R 中的一个真理想，则自然映射 $\pi: R\to R/I$ 诱导出一个从包含 I 的所有中间理想 J(即 $I\subseteq J\subseteq R$)构成的集合，到 R/I 中的所有理想构成的集合且保包含关系的双射 π'

$$\pi': J\mapsto J/I=\{a+I: a\in J\}.$$

因此商环 R/I 的每一个理想具有形式 J/I，对某个唯一的中间理想 J.

证明 若暂时不考虑乘法，则交换环 R 是一个加法阿贝尔群，而它的理想 I 是一个(正规的)子群. 应用群的对应定理(定理 2.123)，即有一个保包含关系的双射

$$\pi_*: \{R\text{ 的包含 } I \text{ 的子群全体}\}\to\{R/I\text{ 的子群全体}\},$$

其中 $\pi_*(J)=J/I$.

若 J 是一个理想，则 $\pi_*(J)$也是一个理想，因为若 $r\in R$，$a\in J$，则 $ra\in J$，故

$$(r+I)(a+I)=ra+I\in J/I.$$

令 π'为π_*在中间理想构成的集合上的限制，则 π'是一个单射，因为 π_*是一个双射. 下面证明 π'是一个满射. 令 J^* 是 R/I 的一个理想，则由习题 3.47，$\pi^{-1}(J^*)$是 R 中的一个中间理想[它包含了 $I=\pi^{-1}(\{0\})$]. 从而由引理 2.14 可知，$\pi'(\pi^{-1}(J^*))=\pi^{-1}(J^*)/I=\pi(\pi^{-1}(J^*))=J^*$. 因此若 $J=\pi^{-1}(J^*)$，则 $J^*=J/I$ ■

例 7.2 令 $I=(m)$为$\mathbb{Z}$中的一个非零理想．$\mathbb{Z}$中每一个理想 J 都是主理想，不妨设 $J=(a)$．易见$(m)\subseteq(a)$当且仅当 $a\mid m$．由对应定理，$\mathbb{I}_m$ 中每个理想都有形式$([a])$，a 为 m 的某个因子． ◀

现在我们来引入两种特别相关的理想：素理想，它与欧几里得引理有关，以及极大理想．

定义 交换环 R 中一个理想 I 称为一个**素理想**若它是一个真理想，即 $I\neq R$，且 $ab\in I$ 能推出 $a\in I$ 或 $b\in I$.

例 7.3 (i)回忆到，一个非零交换环 R 是一个整环当且仅当在 R 中，$ab=0$ 能推出 $a=0$ 或 $b=0$．因此$\{0\}$是 R 的一个素理想当且仅当 R 是一个整环． 519

(ii)我们断言$\mathbb{Z}$中的素理想正好就是理想(p)，其中 $p=0$ 或 p 是一个素数．因为 m 和 $-m$ 生成同一个主理想，所以我们只考虑非负的生成元．若 $p=0$，那么由(i)可得结论成立，因为$\mathbb{Z}$是一个整环．若 p 是一个素数，我们首先证(p)是一个真理想．若不然，$1\in(p)$，则存在一个整数 a 使得 $ap=1$，矛盾．其次，若 $ab\in(p)$，则 $p\mid ab$．由欧几里得引理有 $p\mid a$ 或 $p\mid b$．即 $a\in(p)$或 $b\in(p)$．因此(p)是一个素理想．

反之，若 $m>1$ 不是一个素数，则它有分解 $m=ab$，其中 $0<a<m$ 且 $0<b<m$．因此 a，b 均不为 m 的倍数，从而 a，b 均不属于(m)，所以(m)不是一个素理想． ◀

上例中的证明在更一般的情形中都是成立的．

命题 7.4 设 k 是一个域，则$(p(x))$是一个素理想当且仅当或者 $p(x)=0$ 或者非零多项式 $p(x)\in k[x]$是不可约的．

证明 若非零多项式$(p(x))$不是不可约的，则有分解式

$$p(x)=a(x)b(x),$$

其中 $\deg(a)<\deg(p)$，$\deg(b)<\deg(p)$．因为每一个非零多项式 $g(x)\in(p)$都有形式 $g(x)=d(x)p(x)$对某个 $d(x)\in k[x]$．我们有 $\deg(g)\geqslant\deg(p)$．从而 $a(x)$和 $b(x)$均不属于(p)，故(p)不是一个素理想．

反过来，若 $p(x)=0$，则$(p(x))=\{0\}$，它是一个素理想(因为 $k[x]$是一个整环)．假设 $p(x)$是不可约的．首先，(p)是一个真理想，否则 $R=(p)$，从而 $1\in(p)$，故存在一个多项式 $f(x)$使得 $1=p(x)f(x)$．但 $p(x)$的次数至少为 1，而

$$0=\deg(1)=\deg(pf)=\deg(p)+\deg(f)\geqslant\deg(p)\geqslant 1.$$

此矛盾表明(p)是一个素理想．

其次，若 $ab\in(p)$，则 $p\mid ab$．故由 $k[x]$中的欧几里得引理可得：$p\mid a$ 或 $p\mid b$．因此 $a\in(p)$或 $b\in(p)$，从而(p)是一个素理想． ■

命题 7.5 交换环 R 中一个真理想 I 是素理想当且仅当 R/I 是一个整环．

证明 令 I 是一个素理想．因为 I 是一个真理想，我们有 $1\notin I$，故在 R/I 中，$1+I\neq 0+I$．若 $0=(a+I)(b+I)=ab+I$，则 $ab\in I$．因为 I 是一个素理想，故有 $a\in I$ 或 $b\in I$，即有 $a+I=0$ 或 $b+I=0$．因此 R/I 是一个整环．反之一样易证． ■

下面是相关的第二种理想． 520

定义 交换环 R 中的一个真理想 I 称为一个**极大理想**若不存在理想 J 满足 $I\subsetneq J\subsetneq R$.

因此若 I 是交换环 R 中的一个极大理想且 J 是满足 $I\subseteq J$ 的一个真理想，则 $I=J$.

多项式环 $k[x_1, \cdots, x_n]$的素理想可能非常复杂，但当 k 是代数闭域时，希尔伯特零点定理(定理 7.45)告诉我们，它的每一个极大理想具有如下形式$(x_1-a_1, \cdots, x_n-a_n)$，对某$(a_1, \cdots, a_n)\in k^n$.

我们用现在的术语来重新叙述一下命题 3.43.

引理 7.6 *理想$\{0\}$在交换环 R 中是一个极大理想当且仅当 R 是一个域.*

证明 在命题 3.43 中我们已经证明了，R 中每一个非零理想 I 等于 R 本身当且仅当 R 中每一个非零元都是一个单位. 也就是，$\{0\}$是一个极大理想当且仅当 R 是一个域. ■

命题 7.7 *交换环 R 上的一个真理想 I 是一个极大理想当且仅当 R/I 是一个域.*

证明 由环的对应定理，I 是一个极大理想当且仅当 R/I 除$\{0\}$和它自己之外无其他理想. 由引理 7.6，此性质成立当且仅当 R/I 是一个域. ■

推论 7.8 *交换环 R 上的每一个极大理想都是一个素理想.*

证明 若 I 是一个极大理想，则 R/I 是一个域. 因为每一个域都是一个整环，故 R/I 是一个整环，从而 I 是一个素理想. ■

例 7.9 上面推论的逆命题是不成立的. 例如，考虑$\mathbb{Z}[x]$上的主理想(x). 由习题 3.93 有

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z};$$

因为$\mathbb{Z}$是一个整环，所以(x)是一个素理想. 因为$\mathbb{Z}$不是一个域，所以(x)就不是一个极大理想.

给出一个严格包含(x)的真理想 J 并不难. 令

$$J = \{f(x) \in \mathbb{Z}[x] : f(x) \text{ 的常数项为偶数}\}.$$

521 因为$\mathbb{Z}[x]/J\cong \mathbb{F}_2$，是一个域，故 J 是一个包含(x)的极大理想. ◀

推论 7.10 *若 k 是一个域，则$(x_1-a_1, \cdots, x_n-a_n)$是 $k[x_1, \cdots, x_n]$中的一个极大理想，其中 $a_i\in k$，$i=1, \cdots, n$.*

证明 由定理 3.33，存在唯一的同态

$$\varphi: k[x_1,\cdots,x_n] \to k[x_1,\cdots,x_n]$$

使得 $\varphi(c)=c$，其中 $c\in k$ 且对所有的 i 有 $\varphi(x_i)=x_i-a_i$. 易见 φ 是一个同构，因为它的逆对所有 i 将$x_i\mapsto x_i+a_i$. 由此得出 I 在 $k[x_1, \cdots, x_n]$中是一个极大理想当且仅当 $\varphi(I)$是一个极大理想. 但是$(x_1, \cdots, x_n)$是一个极大理想，因为 $k[x_1, \cdots, x_n]/(x_1, \cdots, x_n)\cong k$ 是一个域. 因此$(x_1-a_n, \cdots, x_n-a_n)$是一个极大理想. ■

当 R 是一个主理想整环(PID)时，推论 7.8 的逆也是成立的.

定理 7.11 *若 R 是一个主理想整环(PID)，则每一个非零素理想 I 都是极大理想.*

证明 假设有一个满足 $I\subseteq J$ 的真理想 J. 因为 R 是一个主理想整环，故存在 $a, b\in R$ 使得 $I=(a)$，$J=(b)$. 由 $a\in J$ 可得 $a=rb$，$r\in R$. 故 $rb\in I$. 但 I 为一个素理想，故有 $r\in I$ 或 $b\in I$. 若 $r\in I$，则 $r=sa$，其中 $s\in R$，故 $a=rb=sab$. 因为 R 为一个整环，故有 $1=sb$. 由习题 3.24 知，$J=(b)=R$，这与 J 是一个真理想相矛盾. 若 $b\in I$，则 $J\subseteq I$. 故 $J=I$. 所以 I

是一个极大理想. ■

下面我们可以给出命题 3.112 的第二种证明.

推论 7.12 *若 k 是一个域且 $p(x)\in k[x]$ 是不可约的，则商环 $k[x]/(p(x))$ 是一个域.*

证明 因为 $p(x)$ 是不可约的，故由命题 7.4 可知，主理想 $I=(p(x))$ 是一个非零的素理想. 因为 $k[x]$ 是一个主理想整环(PID)，故 I 是一个极大理想，从而 $k[x]/I$ 是一个域. ■

每一个交换环 R 是否都包含一个极大理想? 此问题的(肯定的)回答牵涉到*佐恩引理*. 佐恩(Zorn)引理是一个与选择公理等价的定理，在后续的课程里我们将会讨论它(见推论 7.27).

习题

H 7.1 判断对错并给出理由.

(i)若 R 是一个交换环，I 是 R 中的一个理想，不考虑它们的乘法且对(加法)群 R 和 R/I 应用对应定理. R 的包含 I 的且在 R 中是理想的子群对应于 R/I 的在 R/I 中是理想的子群. 522

(ii)若 R 是一个交换环，I 是 R 中的一个理想，不考虑它们的乘法且对(加法)群 R 和 R/I 应用对应定理. R 的包含 I 的且在 R 中不是理想的子群对应于 R/I 的在 R/I 中不是理想的子群.

(iii)若 I 是交换环 R 中的一个理想，$ab\in I$，其中 a，$b\in R$，则 $a\in I$ 或者 $b\in I$.

(iv)若 I 是交换环 R 中的一个理想，$a^2\in I$，其中 $a\in R$，则 $a\in I$.

(v)若 k 是一个域且 $p(x)\in k[x]$ 是不可约的，则 $(p(x))$ 是 $k[x]$ 中一个素理想.

(vi) $\mathbb{Z}$ 中的每一个素理想都是极大理想.

(vii)若 R 是一个交换环，k 是一个域，且 $\varphi: R\to k$ 是一个同态，则 $\ker\varphi$ 是一个极大理想.

(viii)若 R 是一个交换环，k 是一个域，且 $\varphi: R\to k$ 是一个同态，则 $\ker\varphi$ 是一个素理想.

(ix)若 R 是一个交换环，k 是一个域，且 $\varphi: R\to k$ 是一个满同态，则 $\ker\varphi$ 是一个极大理想.

(x) $(x, y-1, z+1)$ 是 $\mathbb{F}_3[x, y, z]$ 中的一个极大理想.

7.2 (i)求 $\mathbb{Z}$ 中的所有的极大理想.

(ii)求 $k[x]$ 中的所有的极大理想，其中 k 是一个域.

(iii)求 $k[[x]]$ 中的所有的极大理想，其中 k 是一个域.

H 7.3 已知布尔环是一个满足对所有 $a\in R$ 均有 $a^2=a$ 的交换环 R. 试证，布尔环中的每一个素理想都是一个极大理想.

*7.4 (i)举一个交换环的例子，使得它包含两个素理想 P 和 Q，且 $P\cap Q$ 不是一个素理想.

(ii)若 $P_1\supseteq P_2\supseteq\cdots\supseteq P_n\supseteq P_{n+1}\supseteq\cdots$ 是交换环 R 中的一个素理想的降序列，试证 $\bigcap_{n\geq 1} P_n$ 是一个素理想.

7.5 令 $f: R\to S$ 为一个环同态.

(i)若 Q 是 S 中的一个素理想，证明 $f^{-1}(Q)$ 是 R 中的一个素理想. 由此得出结论：在对应定理中，若 J/I 是 R/I 中的一个素理想，其中 $I\subseteq J\subseteq R$，则 J 是 R 中的一个素理想.

H (ii)举例说明，若 P 是 R 中的一个素理想，则 $f(P)$ 不一定是 S 中的一个素理想.

7.6 设 k 是一个域，$a=(a_1, \cdots, a_n)\in k^n$. 定义**赋值映射** $e_a: k[x_1, \cdots, x_n]\to k$ 为 $e_a: f(x_1, \cdots, x_n)\mapsto f(a)=f(a_1, \cdots, a_n)$.

(i)通过证明 e_a 是一个满射来证明 $\ker e_a$ 是 $k[x_1, \cdots, x_n]$ 中的一个极大理想.

(ii)通过证明 $\ker e_a=(x_1-a_1, \cdots, x_n-a_n)$ 来证明 $(x_1-a_1, \cdots, x_n-a_n)$ 是 $k[x_1, \cdots, x_n]$ 中的一个极大理想(这是推论 7.10 的第二个证明).

7.7 (i)求 $k[x]$ 中的所有的极大理想，其中 k 是一个代数闭域.

(ii)求$\mathbb{R}[x]$中的所有的极大理想.

(iii)设 k 是一个代数闭域. 试证由 $a\mapsto(x-a)$给出的

$$k\to\{k[x]\text{ 中的极大理想全体}\}$$

523 的函数是一个双射，其中$(x-a)$是 $k[x]$中由 $x-a$ 生成的主理想.

7.8 (i)试证，若对某 i，$x_i-b\in(x_1-a_1,\cdots,x_n-a_n)$，其中 k 是一个域且 $b\in k$，则 $b=a_i$.

(ii)试证由

$$\mu:(a_1,\cdots,a_n)\mapsto(x_1-a_1,\cdots,x_n-a_n)$$

给出的函数 $\mu:k^n\to\{k[x_1,\cdots,x_n]$的极大理想全体$\}$是一个单射. 试举一个使 μ 不是满射的域 k 的例子.

7.9 试证，若 P 是交换环 R 上的一个素理想且 $r^n\in P$，其中 $r\in R$，$n\geqslant 1$，则有 $r\in P$.

7.10 试证$\mathbb{Q}[x,y,z]$上的理想(x^2-2,y^2+1,z)是一个真理想.

7.11 称交换环 R 的一个非空子集 S 是**乘法闭的**若 $0\notin S$ 且若 s，$s'\in S$，则 $ss'\in S$. 试证满足性质 $I\cap S=\varnothing$的理想中的极大者 I 是一个素理想(这样的 I 的存在性可用佐恩引理证明).

*7.12 (i)若 I 和 J 是交换环 R 中的理想，则定义

$$IJ=\left\{\sum_\ell a_\ell b_\ell:a_\ell\in I,b_\ell\in J\right\}.$$

试证 IJ 是 R 中的一个理想且 $IJ\subseteq I\cap J$.

(ii)令 $R=k[x,y]$，其中 k 是一个域，且 $I=(x,y)=J$. 试证 $I^2=IJ\subsetneq I\cap J=I$.

7.13 设 P 是交换环 R 中的一个素理想. 试证，若存在 R 中的理想 I 和 J 使得 $IJ\subseteq P$，则 $I\subseteq P$ 或 $J\subseteq P$.

7.14 设 I 和 J 是交换环 R 的主理想，定义**冒号理想**

$$(I:J)=\{r\in R:rJ\subseteq I\}.$$

(i)试证$(I:J)$是一个包含 I 的理想.

(ii)令 R 是一个整环，a，$b\in R$，其中 $b\neq 0$. 若 $I=(ab)$，$J=(b)$. 试证$(I:J)=(a)$.

7.15 令 I 和 J 是交换环 R 中的理想.

(i)试证 $\varphi:r\mapsto(r+I,r+J)$是 $R/(I\cap J)\to(R/I)\times(R/J)$的一个单射.

H (ii)称 I 和 J 是**互素的**若 $I+J=R$. 试证若 I 和 J 是互素的，则环同态 $\varphi:R/(I\cap J)\to(R/I)\times(R/J)$是一个同构.

(iii)设 R 是一个交换环，$I_1,\cdots,I_n$ 是两两互素的理想，即对所有 $i\neq j$，I_i 和 I_j 是互素的. 试证

$$R/(I_1\cap\cdots\cap I_n)\cong(R/I_1)\times\cdots\times(R/I_n).$$

(iv)下面来推广**中国剩余定理**. 设 R 是一个交换环，$I_1,\cdots,I_n$ 是两两互素的理想. 试证若 $a_1,\cdots,a_n\in R$，则对所有的 i，存在 $r\in R$ 使得 $r+I_i=a_i+I_i$.

7.16 一个交换环 R 称为**局部环**若它有唯一的一个极大理想.

(i)若 p 是一个素数. 试证

$$\{a/b\in\mathbb{Q}:p\nmid b\}$$

524 是一个局部环.

(ii)若 k 是一个域，试证 $k[[x]]$是一个局部环.

H (iii)设 R 是一个局部环，且有唯一的极大理想 M. 试证 $a\in R$ 是一个单位当且仅当 $a\notin M$.

7.2 唯一分解

我们已经证明了$\mathbb{Z}$中及 $k[x]$(其中 k 是一个域)中的唯一分解定理. 事实上，我们证明了这

两个结果的一个共同的推广：每一个欧氏环都有唯一分解. 我们现在的目标是再推广此结果. 首先将其推广至一般的主理想整环(PID)上，然后再推广至 $R[x]$上，其中 R 是一个具有唯一分解的环. 由此得出一个域 k 上的多变量的多项式环 $k[x_1, \cdots, x_n]$中有唯一分解，由此立即可得，两个多变量的多项式有最大公因式.

我们先推广一些早先给出的定义. 回忆到交换环 R 中元素 a 和 b 称为是**相伴元**若存在一个单位 $u\in R$ 使得 $b=ua$. 例如，在$\mathbb{Z}$ 中，单位是± 1，故整数 m 的相伴元只能为$\pm m$. 在 $k[x]$中，其中 k 是一个域，单位是非零的常数，故多项式 $f(x)\in k[x]$的相伴元只能是 $uf(x)$，其中 $u\in k$ 且 $u\neq 0$. $\mathbb{Z}[x]$中的单位只有± 1，故多项式 $f(x)\in\mathbb{Z}[x]$的相伴元只能是$\pm f(x)$.

考虑交换环 R 中的两个主理想(a)和(b). 易见下列是等价的：$b\mid a$；$a\in(b)$；对某 $r\in R$ 有 $a=rb$；$(a)\subseteq(b)$. 当 R 是一个整环时，我们有进一步的结论.

命题 7.13 令 R 是一个整环，a，$b\in R$.

(i)$a\mid b$ 且 $b\mid a$ 当且仅当 a 和 b 是相伴元.

(ii)主理想(a)和(b)是相等的当且仅当 a 和 b 是相伴元.

(iii)$(a)\subseteq(b)$当且仅当 $b\mid a$，即对某 $c\in R$，$a=cb$. 包含关系是真的，$(a)\subsetneq(b)$当且仅当 b 是 a 的真因子，即 c 和 b 都不是单位.

证明 (i)这就是命题 3.15.

(ii)若$(a)=(b)$，则$(a)\subseteq(b)$且$(b)\subseteq(a)$. 因此 $a\in(b)$且 $b\in(a)$. 所以 $a\mid b$ 且 $b\mid a$. 由(i)知，a 和 b 是相伴元. 易证反之也成立，我们甚至可以不必假设 R 是一个整环就可得到这个结论.

(iii)若 $b\mid a$，则对某 $c\in R$ 有 $a=cb$. 若 $x\in(a)$，则对某 $r\in R$ 有 $x=ra=rcb\in(b)$，所以$(a)\subseteq(b)$. 反之，若$(a)\subseteq(b)$，则 $a\in(b)$且 $a=cb$，因此 $b\mid a$. 525

假设$(a)\subsetneq(b)$，所以 $a=cb$. 若 c 是一个单位，则 a 和 b 是相伴元. 因此由(i)有$(a)=(b)$，这是一个矛盾. 若 b 是一个单位，则 a 也是一个单位. 但是任意两个单位是相伴元，所以 a 和 b 是相伴元，又矛盾！因此 b 是 a 的真因子.

反之，假设 b 是 a 的真因子. 由 $b\mid a$ 有包含关系$(a)\subseteq(b)$. 若此关系不为真，则$(a)=(b)$，从而 a 和 b 是相伴元. 但是读者容易证明，a 的真因子不是 a 的相伴元，所以$(a)\subsetneq(b)$. ■

$\mathbb{Z}$ 中的素数和 $k[x]$中的不可约多项式(其中 k 是一个域)这两个概念有一个共同的推广.

定义 交换环 R 中一个元素 p 称为是**不可约的**若它既不是零元也不是一个单位，且它仅有的因子是单位或 p 的相伴元.

因此，若 $p\in R$ 既不是零元又不是一个单位，则 p 是不可约的当且仅当它没有真因子. 例如，$\mathbb{Z}$ 中的不可约元是$\pm p$，其中 p 是素数；在 $k[x]$中(其中 k 是一个域)不可约元是不可约多项式 $p(x)$，即 $\deg(p)\geqslant 1$ 且 $p(x)$没有满足 $\deg(f)<\deg(p)$和 $\deg(g)<\deg(p)$的分解$p(x)=f(x)g(x)$. 当 R 不是域时，环 $R[x]$中的不可约多项式不保持这个特性. 例如，在$\mathbb{Z}[x]$中，多项式 $f(x)=2x+2$ 不能分解成两个次数比 $\deg(f)=1$ 还小的多项式的乘积，但$f(x)$不是不可约元，因为 $f(x)$有分解 $f(x)=2x+2=2(x+1)$，2 和 $x+1$ 均不是单位.

定义 若 R 是一个交换环，则 R 中元素 r 称为是**不可约元的乘积**若它既不是零元又不是

一个单位，且存在不可约元 p_1，…，p_n 使得 $r=p_1\cdots p_n$，其中 $n\geqslant 1$.

当 $n=1$ 时，它就是不可约元的定义. R 中的每一个不可约的元素都是不可约元(它是一个因子的乘积)的乘积.

下面就是我们一直在寻找的定义.

定义 整环 R 称为是一个**唯一分解整环**(简记为 **UFD**)，若

(i)R 中每一个非 0 也非单位的元或者是不可约的或者是不可约元的乘积；

(ii)若 $p_1\cdots p_m=q_1\cdots q_n$，其中 p_i 和 q_j 是不可约元，则 $m=n$ 且存在一个置换 $\sigma\in S_n$ 使得对所有的 i 有 p_i 和 $q_{\sigma(i)}$ 是相伴元.

当我们证明$\mathbb{Z}$ 和 $k[x]$(其中 k 为一个域)具有不可约元的唯一分解时，我们没有提及相伴元，这是因为在每一种情形下，一般的不可约元总是被它的适当选择的相伴元所代替. 在$\mathbb{Z}$

526 中，我们选择了正的不可约元(即素数)；在 $k[x]$中，我们选择了首一多项式. 例如，读者应该看出，“$\mathbb{Z}$ 是一个 UFD”这个命题就是算术基本定理的一个重述.

每一个 PID 是一个 UFD 的证明要用一个新的概念：理想链.

引理 7.14 若 R 是一个交换环.

(i)若

$$I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq I_{n+1}\subseteq\cdots$$

是 R 中的一个上升的理想链，则 $\bigcup_{n=1}^{\infty} I_n$ 是一个理想.

(ii)若 R 是一个 PID，则不存在无限严格升的理想链

$$I_1\subsetneq I_2\subsetneq\cdots\subsetneq I_n\subsetneq I_{n+1}\subsetneq\cdots.$$

(iii)若 R 是一个 PID，设 $r\in R$ 是非 0 也非单位的元，则 r 是不可约的或者是不可约元的乘积.

证明 (i)定义 $J=\bigcup_{n=1}^{\infty} I_n$. 若 $a\in J$，则 $a\in I_n$，对某 n. 若 $r\in R$，则 $ra\in I_n$，因为 I_n 是一个理想，因此 $ra\in J$. 若 a，$b\in J$，则存在理想 I_n 和 I_m 使得 $a\in I_n$ 和 $b\in I_m$. 因为此链是上升的，所以我们可以假设 $I_n\subseteq I_m$，故 a，$b\in I_m$. 因为 I_m 是一个理想，所以 $a-b\in I_m$，故 $a-b\in J$. 从而 J 是一个理想.

(ii)相反地，假设存在一个无限严格升的理想链，则定义 $J=\bigcup_{n=1}^{\infty} I_n$. 由(i)可知 J 是一个理想. 因为 R 是一个 PID，所以我们有 $J=(d)$，对某 $d\in J$. 又 d 一定落在某个 I_n 中，因此

$$J=(d)\subseteq I_n\subsetneq I_{n+1}\subseteq J,$$

这是一个矛盾.

(iii)称一个非零非单位的元 $a\in R$ 是好的若它是不可约的或是不可约元的乘积，否则称为坏的. 我们一定要证明不存在坏的元素. 若 a 是坏的，则它不是不可约元，故 $a=rs$，这里 r，s 均是真因子. 但好的元的乘积还是好的，所以至少有一个因子是坏的，不妨设为 r. 由命题 7.13(iii)知$(a)\subsetneq(r)$. 由归纳可得，存在坏的元的一个序列 $a=a_1$，$r=a_2$，…，a_n，…，其中每个 a_{n+1}都是 a_n 的一个真因子. 此序列产生一个严格上升的链

$$(a_1)\subsetneq(a_2)\subsetneq\cdots\subsetneq(a_n)\subsetneq(a_{n+1})\subsetneq\cdots,$$

这与(ii)矛盾. ■

命题 7.15 假设 R 是一个整环，且 R 中每个非零非单位的元 r 均为不可约的或不可约元的乘积. 则 R 是一个 UFD 当且仅当对每一个不可约元 $p\in R$，(p)是 R 中的一个素理想. 527

证明 假设 R 是一个 UFD. 若 a，$b\in R$ 且 $ab\in(p)$，则存在 $r\in R$ 使得

$$ab = rp.$$

将 a，b，r 均分解成不可约元的乘积. 由唯一分解性可知，等式的左边一定有 p 的一个相伴元，此相伴元是 a 或 b 的一个因子，因此有 $a\in(p)$或 $b\in(p)$.

反之的证明只须稍为改动一下算术基本定理的证明. 假设

$$p_1\cdots p_m = q_1\cdots q_n, \tag{1}$$

其中 p_i 和 q_j 均为不可约元. 我们对 $\max\{m, n\}\geqslant 1$ 用归纳法来证明 $n=m$ 且重新编号后，对所有 i 有 q_i 和 p_i 是相伴元. 基础步骤是 $\max\{m, n\}=1$，故 $p_1=q_1$，结论显然成立. 考虑归纳步骤，由给定的等式知 $p_1 \mid q_1\cdots q_n$. 由假设，(p_1)是一个素理想，存在某 q_j 使得 $p_1\mid q_j$(它类似于欧几理得引理). 但作为一个不可约元，q_j 除单位及相伴元外无其他因子，所以 q_j 和 p_1 是相伴元：$q_j=up_1$，u 是一个单位. 在等式(1)两边消去 p_1，我们有 $p_2\cdots p_m=uq_1\cdots\widehat{q_j}\cdots q_n$. 由归纳假设，$m-1=n-1$(所以 $m=n$)，且适当编号后，对所有 i，q_i 和 p_i 是相伴元. ∎

定理 7.16 若 R 是一个 PID，则 R 是一个 UFD. 特别地，每一个欧氏环是一个 UFD.

证明 考虑到前面两个结果，只须证明当 p 是一个不可约元时，(p)是一个素理想. 假设存在一个真理想 I 使得$(p)\subsetneq I$. 因为 R 是一个 PID，所以 $I=(b)$，对某 $b\in R$，且 b 不是一个单位. 由命题 7.13(iii)，b 为 p 的真因子，这与 p 为不可约元矛盾. 故(p)是一个极大理想，从而为一个素理想. ∎

回忆到，gcd(最大公因子)这个概念是可以定义在任何一个交换环中的.

定义 令 R 是一个交换环，a_1，…，$a_n\in R$. a_1，…，a_n 的**公因子**是指满足对所有的 i，$c\mid a_i$ 的元素 $c\in R$. a_1，…，a_n 的**最大公因子**或 gcd 指的是满足对所有公因子 c，都有 $c\mid d$ 的公因子 d.

甚至在我们熟悉的例子中，如$\mathbb{Z}$ 和 $k[x]$，gcd 并不是唯一的，除非另外附加条件. 例如在$\mathbb{Z}$ 中，若 d 是上面定义的一对整数的 gcd，则 $-d$ 也是一个 gcd. 为使 gcd 唯一，人们定义$\mathbb{Z}$ 中的非零的 gcd 为一个正数. 类似地，在 $k[x]$中(k 为一个域)，人们加了如下条件：非零的 gcd 是一个首一多项式. 然而在一般的 PID 中，元素可能没有适当的相伴元. 528

设 R 是一个整环，易见若 d 和 d'为元素 a_1，…，a_n 的 gcd，则 $d\mid d'$且 $d'\mid d$. 由命题 7.13 可知，d 和 d'是相伴元，因此$(d)=(d')$. 所以若 gcd 存在的话，则是不唯一的，但它们都生成同一个主理想.

在习题 3.81 中我们看到，存在一个整环 R，它包含一对无 gcd 的元素. 我们现在来证明在 UFD 中 gcd 总是存在的.

命题 7.17 设 R 是一个 UFD，则 R 中的任一组元素 a_1，…，a_n 的 gcd 均存在.

证明 只须证明任两个元素 a，b 的 gcd 存在即可，因为应用归纳法能很容易地得到任意有限个元素的 gcd 存在的证明. 我们修改命题 1.55 的证明.

存在单位 u，v 及不同的不可约元 p_1，…，p_t 使得

$$a = up_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$$

及

$$b = vp_1^{f_1}p_2^{f_2}\cdots p_t^{f_t},$$

其中对所有的 i，$e_i \geqslant 0$，$f_i \geqslant 0$(像通常一样，允许一些指数为零，使得我们在两个分解式中应用相同的不可约元因子)．易见，若 $c \mid a$，则 c 分解为不可约元的乘积的形式为 $c = wp_1^{g_1}p_2^{g_2}\cdots p_t^{g_t}$，其中 w 为一个单位，对所有 i 有 $g_i \leqslant e_i$．因此 c 是 a 和 b 的公因子当且仅当 $g_i \leqslant m_i$，对所有的 i，其中

$$m_i = \min\{e_i, f_i\}.$$

显然 $p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$ 是 a 和 b 的一个 gcd. ■

我们提醒读者注意，我们没有证明元素 a_1，…，a_n 的一个 gcd 是它们的一个线性组合．事实上，这是不正确的(参见习题 7.23)．

定义 一个 UFD 中元素 a_1，…，a_n 称为**互素的**，若 a_1，…，a_n 的每一个公因子都是一个单位．

我们下面来证明，若 R 是一个 UFD，则 $R[x]$也是．这个定理是高斯发现的，其证明用了高斯定理(定理 3.96)中的思想．由此可得，若 k 是一个域，则 $k[x_1, \cdots, x_n]$是一个 UFD.

定义 多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0 \in R[x]$，其中 R 是一个 UFD，称为**本原的**若它的系数是互素的，即 a_n，…，a_1，a_0 的公因子是单位．

若 $f(x)$不是本原的，则存在不可约元 $q \in R$ 整除 $f(x)$的每一个系数，因为若 gcd 是一个
529 非单位的元 d，则取 q 为 d 的任一个不可约元因子即可．

例 7.18 我们现在来证明，若 R 是一个 UFD，则每一个正次数的不可约元 $p(x) \in R[x]$都是本原的．若不然，则存在一个不可约元 $q \in R$ 使得 $p(x)=qg(x)$．因为 $p(x)$是 $R[x]$中的不可约元，所以它的因子是 $R[x]$中的单位或相伴元．注意，q 是 R 中的不可约元，它可能是 $R[x]$中的单位吗？若存在 $f \in R[x]$使得 $qf=1$，则 $0=\deg(1)=\deg(qf)=\deg(q)+\deg(f)$，因此$\deg(f)=0$，$f \in R$．故 q 一定是 R 中的单位，与它是 R 中的不可约元相违．因此 q 一定是 $p(x)$的一个相伴元．但是 $R[x]$中相伴元具有相同的次数(因为单位的次数为零)，因此 $\deg(p)=0$，与$p(x)$次数为正的矛盾．由此得出 $p(x)$是本原的． ◀

下面是高斯引理(定理 3.92)的一个推广．

引理 7.19 若 R 是一个 UFD，$f(x)$，$g(x) \in R[x]$都是本原的，则它们的乘积 $f(x)g(x)$也是本原的．

证明 相反地，假设 $f(x)g(x)$不是本原的，则存在一个不可约元 p，它能整除 $f(x)g(x)$的所有系数．设 $\pi: R \to R/(p)$是自然映射 $\pi: a \mapsto a+(p)$．由定理 3.33，存在一个环同态 $\tilde{\pi}: R[x] \to (R/(p))[x]$，它将多项式的每个系数 c 换成$\pi(c)$．$f(x)g(x)$不是本原的就是说，在$(R/(p))[x]$中，$0=\tilde{\pi}(fg)=\tilde{\pi}(f)\tilde{\pi}(g)$．因为$(p)$是一个素理想，所以 $R/(p)$是一个整环．因此$(R/(p))[x]$也是一个整环．但由 f 和 g 都是本原的可知，在$(R/(p))[x]$中，$\tilde{\pi}(f)$和$\tilde{\pi}(g)$均不是 0．这就与$(R/(p))[x]$是一个整环矛盾． ■

定义 若 R 是一个 UFD，$f(x)=a_nx^n+\cdots+a_1x+a_0 \in R[x]$．定义 $c(f) \in R$ 为 a_n，…，

a_1，a_0 的一个 gcd. 称 $c(f)$ 为 $f(x)$ 的**容度**.

注意一个多项式 $f(x)$ 的容度是不唯一的，但 $f(x)$ 的任两个容度是相伴元. 当 UFD 上一个多项式 $f(x)$ 被给定，则 $c(f)$ 表示 f 的任意一个容度.

引理 7.20 令 R 为一个 UFD.

(i)每一个非零的 $f(x)\in R[x]$ 有分解

$$f(x) = c(f)f^*(x),$$

其中 $c(f)\in R$ 是 $f(x)$ 的一个容度且 $f^*(x)\in R[x]$ 是本原的.

(ii)此分解在下面意义下是唯一：若 $f(x)=dg^*(x)$，其中 $d\in R$，$g^*(x)\in R[x]$ 是本原的，则 d 和 $c(f)$ 是相伴元，而 $f^*(x)$ 和 $g^*(x)$ 也是相伴元. 530

(iii)设 $g^*(x)$，$f(x)\in R[x]$. 若 $g^*(x)$ 是本原的且 $g^*(x)\mid bf(x)$，其中 $b\in R$，则 $g^*(x)\mid f(x)$.

证明 (i)若 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 且 $c(f)$ 是 f 的容度，则对 $i=0$，1，…，n，在 R 中有分解 $a_i=c(f)b_i$. 若我们定义 $f^*(x)=b_nx^n+\cdots+b_1x+b_0$，则 $f^*(x)$ 是本原的且 $f(x)=c(f)f^*(x)$.

(ii)为证明唯一性，只须证明 $c(f)$ 和 d 都是 $f(x)$ 的系数 a_n，…，a_1，a_0 的 gcd，因为这样的话它们就是相伴元. 由此得出 $g^*(x)$ 和 $f^*(x)$ 就是相伴元：若 $d=uc(f)$，其中 u 是一个单位，则 $c(f)f^*=f=dg^*=uc(f)g^*$ 且 $f^*=ug^*$.

假设 $f(x)=dg^*(x)$ 表明 d 是 $f(x)$ 的系数的一个公因子. 注意 $c(f)$ 是 $f(x)$ 的系数的一个 gcd，所以 $c(f)\mid d$. 若 $c(f)$ 是一个真因子，则 $d=rc(f)$，其中 $r\in R$ 不是一个单位. 因此 $f(x)=c(f)f^*(x)=drf^*(x)$. 另一方面，$f(x)=dg^*(x)$，所以 $g^*(x)=rf^*(x)$ 不是本原的. 这与 d 也是 $f(x)$ 的系数的一个 gcd 相矛盾，从而 $c(f)$ 和 d 是相伴元.

(iii)因为 $g^*(x)\mid bf(x)$，所以存在 $h(x)\in R[x]$ 使得

$$bf(x) = g^*(x)h(x) \tag{2}$$

由(i)我们有 $h(x)=c(h)h^*(x)$，其中 h^* 是本原的. 代入(2)中，有

$$bf(x) = c(h)g^*(x)h^*(x).$$

由此得出 b 整除 $c(h)g^*(x)h^*(x)$ 的每一个系数，即 b 是这些系数的一个公因子. 由引理 7.19，$g^*(x)h^*(x)$ 是本原的，故由(ii)，$c(h)$ 是 $c(h)g^*(x)h^*(x)$ 的一个容度，所以 $b\mid c(h)$. 因此 $c(h)=ba$，对某 $a\in R$，且 $bf(x)=c(h)g^*(x)h^*(x)=bag^*(x)h^*(x)$. 消去 b，我们有 $f(x)=ag^*(x)h^*(x)$，亦即 $g^*(x)\mid f(x)$. ■

定理 7.21(高斯) 若 R 是一个 UFD，则 $R[x]$ 也是一个 UFD.

证明 我们首先对 $\deg(f)$ 用归纳法来证明，每一个非零非单位的 $f(x)\in R[x]$ 是不可约元的乘积. 若 $\deg(f)=0$，则 $f(x)$ 是一个常数，因此在 R 中. 因为 R 是一个 UFD，故 f 是不可约元的积. 若 $\deg(f)>0$，则 $f(x)=c(f)f^*(x)$，其中 $c(f)\in R$ 且 $f^*(x)$ 是本原的. 由基础步骤知，$c(f)$ 是一个单位或不可约元的乘积. 若 $f^*(x)$ 是不可约元，则证明已完成. 否则 $f^*(x)=g(x)h(x)$，其中 $g(x)$，$h(x)$ 均不是单位. 因为 $f^*(x)$ 是本原的，g 和 h 不是常量，故它们中的每一个的次数都小于 $\deg(f^*)=\deg(f)$，故由归纳假设，每一个都是不可约元的

531 乘积.

应用命题 7.15：若对每一个不可约元 $p(x)\in R[x]$，$(p(x))$是一个素理想，即若 $p(x)\mid f(x)g(x)$，则 $p(x)\mid f(x)$或 $p(x)\mid g(x)$，则 $R[x]$是一个 UFD. 我们假设 $p(x)\in R[x]$是不可约的，$p(x)\mid f(x)g(x)$但 $p(x)\nmid f(x)$，来证明 $p(x)\mid g(x)$. 在此证明中，$f(x)$有时简记为 f.

情形(i). 假设 $\deg(p)=0$. 记

$$f(x)=c(f)f^{*}(x)\text{ 且 }g(x)=c(g)g^{*}(x),$$

其中 $c(f)$，$c(g)\in R$ 且 $f^{*}(x)$，$g^{*}(x)$是本原的. 由 $p\mid fg$ 有 $p\mid c(f)c(g)f^{*}(x)g^{*}(x)$. 因为 $f^{*}(x)g^{*}(x)$是本原的，由引理 7.20(ii)，我们一定有 $c(f)c(g)$是 $c(fg)$的一个相伴元. 然而，若 $p\mid f(x)g(x)$，则 p 整除 fg 的每一个系数，也就是 p 是 fg 的所有系数的一个公因子，所以在 R 中，$p\mid c(fg)=c(f)c(g)$，而 R 是一个 UFD. 由命题 7.15 知道，(p)是一个 R 中的素理想，故有 $p\mid c(f)$或 $p\mid c(g)$. 若 $p\mid c(f)$，则 $p(x)\mid c(f)f^{*}(x)=f(x)$，矛盾！因此 $p\mid c(g)$，从而 $p\mid g(x)$，得证.

情形(ii). 设 $\deg(p)>0$. 令

$$(p,f)=\{sp+tf : s,t\in R[x]\}.$$

当然，(p,f)是一个包含 $p(x)$，$f(x)$的主理想. 取 $m(x)$为(p,f)中次数最低的多项式. 若 $Q=\mathrm{Frac}(R)$，那么由 $Q[x]$中的除法算式，存在多项式 $q'(x)$，$r'(x)\in Q[x]$使得 $f(x)=m(x)q'(x)+r'(x)$，其中 $r'(x)=0$ 或 $\deg(r')<\deg(m)$. 去掉分母，则存在多项式 $q(x)$，$r(x)\in R[x]$及常量 $b\in R$ 使得

$$bf(x)=q(x)m(x)+r(x),$$

其中 $r(x)=0$ 或 $\deg(r)<\deg(m)$. 因为 $m\in(p,f)$是一个理想，所以 $r=bf-qm\in(p,f)$. 因为 m 是(p,f)中次数最小的项，故一定有 $r=0$，即 $bf(x)=m(x)q(x)$，故 $bf(x)=c(m)m^{*}(x)q(x)$. 但 $m^{*}(x)$是本原的，且 $m^{*}(x)\mid bf(x)$，故由引理 7.20(iii)，有 $m^{*}(x)\mid f(x)$. 类似地，换 $f(x)$为 $p(x)$，可得出 $m^{*}(x)\mid p(x)$. 因为 $p(x)$是既约元，它的因子只有单位和相伴元. 若 $m^{*}(x)$是 $p(x)$的一个相伴元，那么由 $m^{*}(x)\mid m(x)$可推出 $p(x)\mid f(x)$，与假设相违. 因此 $m^{*}(x)$一定是一个单位，即 $m(x)=c(m)\in R$，故(p,f)包含非零的常量 $c(m)$. 由 $c(m)=sp+tf$，故

$$c(m)g=spg+tfg.$$

因为 $p(x)\mid f(x)g(x)$，我们有 $p\mid c(m)g$. 但 $p(x)$是本原的，因为它是不可约元，故由引理 7.20(iii)，$p(x)\mid g(x)$，定理得证. ■

532 由命题 7.17 知，若 R 是一个 UFD，则在 $R[x]$中 gcd 存在.

推论 7.22 若 k 是一个域，则 $k[x_1,\cdots,x_n]$是一个 UFD.

证明 对 $n\geqslant 1$ 用归纳法. 在第 3 章中我们已经证明了一个变量的多项式环 $k[x_1]$是一个 UFD. 下证归纳步骤. 注意到 $k[x_1,\cdots,x_n,x_{n+1}]=R[x_{n+1}]$，其中 $R=k[x_1,\cdots,x_n]$. 由归纳假设，R 是一个 UFD，再由定理 7.21 知 $R[x_{n+1}]$也是一个 UFD. ■

高斯定理，即定理 3.96，可推广如下：

推论 7.23 令 R 是一个 UFD，$Q=\mathrm{Frac}(R)$，$f(x)\in R[x]$. 若在 $Q[x]$中，

$$f(x)=G(x)H(x),$$

则在 $R[x]$中有分解

$$f(x)=g(x)h(x),$$

其中 $\deg(g)=\deg(G)$，$\deg(h)=\deg(H)$. 事实上，在 $Q[x]$中，$g(x)$和 $G(x)$是相伴元，$h(x)$和 $H(x)$也是相伴元.

因此若 $f(x)$在 $R[x]$中不能分解为次数更低的多项式的乘积，则 $f(x)$在 $Q[x]$中是不可约的.

证明 去掉分母，存在 r，$s\in R$ 使得 $rG(x)\in R[x]$且 $sH(x)\in R[x]$. 因此 $rsf(x)=[rG(x)][sH(x)]$是 $R[x]$中的一个分解. 由引理 7.20，在 $R[x]$中，存在分解

$$rsf(x)=c(rG)c(sH)[rG]^*(x)[sH]^*(x),$$

其中$[rG]^*(x)$，$[sH]^*(x)\in R[x]$是本原多项式. 由引理 7.20(ii)，$c(rsf)=c(rG)c(sH)$，故 $rsf(x)=c(rsf)[rG]^*(x)[sH]^*(x)$. 但是$c(f)\in R$ 且$c(rsf)=rsc(f)$，因此在$R[x]$中，$f(x)=c(f)[rG]^*(x)[sH]^*(x)$. 从而在 $R[x]$中有分解 $f(x)=g(x)h(x)$，其中 $g(x)=c(f)[r]^*(x)$且 $h(x)=[sH]^*(x)$. ■

多个变量的多项式的不可约性的判定要比一个变量的多项式的不可约性的判定困难许多. 但有如下的一个法则.

推论 7.24 设 k 是一个域，$f(x_1,\cdots,x_n)$是 $R[x_n]$中的一个本原多项式，其中 $R=k[x_1,\cdots,x_{n-1}]$. 若 f 在 $R[x_n]$中不能分解成两个更低次数的多项式的乘积，则 f 在$k[x_1,\cdots,x_n]$中是不可约的.

证明 为便于我们视 f 为 $R[x_n]$中的多项式，记 $f(x_1,\cdots,x_n)=F(x_n)$(当然 f 的系数是 $k[x_1,\cdots,x_{n-1}]$中的多项式). 假设 $F(x_n)=G(x_n)H(x_n)$. 由假设，G 和 H 的次数(关于 x_n 的)不能均低于 $\deg(F)$，故它们中的一个次数为 0，设为 G. 因为 F 是本原的，由此得出 G 是 $k[x_1,\cdots,x_{n-1}]$中的单位，从而 $f(x_1,\cdots,x_n)$在 $R[x_n]=k[x_1,\cdots,x_n]$中是不可约的. ■

当然，此推论适用于任何一个变量 x_i，不仅仅是 x_n. 533

例 7.25 我们断言 $f(x,y)=x^2+y^2-1\in k[x,y]$是不可约的，其中 k 是一个特征非 2 的域. 记$Q=k(y)=\mathrm{Frac}(k[y])$，视 $f(x,y)\in Q[x]$. 又二次式 $g(x)=x^2+(y^2-1)$在 $Q[x]$中是不可约的当且仅当它在 $Q=k(y)$中无根. 由习题 3.66 知，的确如此.

因为 $k[x,y]$是一个 UFD，由命题 7.15 知(x^2+y^2-1)是一个素理想，因为它是由一个不可约多项式生成的. ◀

习题

H 7.17 判断对错并给出理由.

(i)若 a，b，c 是整环 R 中的元素，若 a 和 b 是相伴元，则 $a\mid c$ 当且仅当 $b\mid c$.

(ii)若 a，b，c 是整环 R 中的元素，若 a 和 b 是相伴元，则 $c\mid a$ 当且仅当 $c\mid b$.

(iii)$\mathbb{Z}$ 是一个 UFD.

(iv)若一个 UFD 中的一个元素 a 有两种不可约元分解，$a=p_1\cdots p_n=q_1\cdots q_m$，则 $m=n$ 且对所有的 i 有 $p_i=q_i$.

(v)若一个 UFD 中的一个元素 a 有两种不可约元分解，$a=p_1\cdots p_n=q_1\cdots q_m$，则 $m=n$ 且 p_i 和 q_i 是相伴.

(vi)若一个 UFD 中的一个元素 a 有两种不可约元分解，$a=p_1\cdots p_n=q_1\cdots q_m$，则 $m=n$ 且存在 $\sigma\in S_n$ 使得 p_i 和 $q_{\sigma}(i)$ 是相伴元，对所有的 i.

(vii)若 R 是一个 PID，则不存在无限下降的理想链 $I_1 \supsetneq I_2 \supsetneq\cdots$.

(viii)若 R 是一个 PID，则 $R[x]$ 是一个 PID.

(ix)若 R 是一个 UFD，则 $R[x]$ 是一个 UFD.

(x)若 R 是一个 PID，则 $R[x]$ 是一个 UFD.

7.18 在任一个交换环 R 中，试证，若任意两个元的 gcd 总存在，则任意有限个元素的 gcd 也存在.

*7.19 设 R 为一个 UFD，$Q=\mathrm{Frac}(R)$ 为它的分式域. 试证每一个非零元 $q\in Q$ 都有一个最简表示：$q=a/b$，其中 a，b 互素.

*7.20 设 R 是一个 UFD，a，b，$c\in R$. 若 a，b 是互素的，且 $a\mid bc$，试证 $a\mid c$.

7.21 设 R 是一个整环，试证 $R[x_1，\cdots，x_n]$ 中的单位仅为 R 中的单位.

7.22 设 R 是一个 UFD，$f(x)$，$g(x)\in R[x]$，试证 $c(fg)$ 和 $c(f)c(g)$ 是相伴元.

*7.23 (i)试证在 $k[x，y]$ 中，x 和 y 是互素的，其中 k 是一个域.

(ii)试证在 $k[x，y]$ 中，1 不是 x 和 y 的一个线性组合.

7.24 试证对所有的 $n\geqslant 1$，$\mathbb{Z}[x_1，\cdots，x_n]$ 是一个 UFD.

7.25 设 k 是一个域，$f(x_1，\cdots，x_n)\in k[x_1，\cdots，x_n]$ 为 $R[x_n]$ 中的一个本原多项式，其中 $R=k[x_1，\cdots，x_{n-1}]$. 设 f 是关于 x_n 的二次或三次多项式，试证 f 在 $k[x_1，\cdots，x_n]$ 中是不可约的当且仅当 f(视为关于 x_n 的多项式)在 $k(x_1，\cdots，x_{n-1})$ 中无根.

7.26 设 $f(x_1，\cdots，x_n)=x_ng(x_1，\cdots，x_{n-1})+h(x_1，\cdots，x_{n-1})$，其中 $(g，h)=1$.

534 (i)试证 f 在 $k[x_1，\cdots，x_n]$ 中是不可约的.

(ii)试证 xy^2+z 是 $k[x，y，z]$ 中的一个不可约多项式.

7.27 **(爱森斯坦判别法)**设 R 是一个 UFD，$Q=\mathrm{Frac}(R)$，$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. 试证，若存在一个既约元 $p\in R$ 使得 $p\mid a_i$，对所有的 $i<n$，但 $p\nmid a_n$ 且 $p^2\nmid a_0$. 则 $f(x)$ 在 $Q[x]$ 中是不可约的.

7.28 试证

$$f(x,y)=xy^3+x^2y^2-x^5y+x^2+1$$

是 $\mathbb{R}[x，y]$ 中的一个不可约多项式.

7.3 诺特环

当 k 是一个域时，$k[x_1，\cdots，x_n]$ 的最重要的性质之一是它中的每一个理想都可由有限个元素生成，这个性质与我们在证明 PID 就是 UFD 的过程中所见过的理想链密切相关.

一个交换环满足升链条件若它的每一个上升的理想链从某项开始后就是固定不变的了.

定义 称一个交换环 R 满足 **ACC，升链条件**，若每一个上升的理想链

$$I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$$

均会停止，即此序列从某项开始后就是**固定不变了**：存在整数 N 使得 $I_N=I_{N+1}=I_{N+2}=\cdots$.

由引理 7.14(ii)的证明知，每一个 PID 都满足 ACC.

下面是一类重要的理想.

定义 交换环 R 中的一个理想 I 称为**有限生成的**若存在有限个元素 $a_1，\cdots，a_n\in I$ 使得

$$I=\left\{\sum_i r_ia_i : r_i\in R,\text{对所有的 } i\right\}.$$

即，I 中每一个元素都是 a_i 的一个线性组合. 记

$$I=(a_1,\cdots,a_n)$$

且称 I 是由 a_1，…，a_n **生成的理想**.

理想 I 的一组生成元 a_1，…，a_n 有时称为 I 的一个**基**，尽管这是一个比向量空间的基更弱的概念，因为没有假设表示的唯一性.

在一个 PID 中，每一个理想 I 都可由一个元素生成，故 I 是有限生成的. 535

命题 7.26 对一个交换环 R 而言，下列条件等价.

(i)R 满足 ACC.

(ii)R 满足**最大条件**：每一个 R 中理想的非空集合 $\mathcal{F}$ 都有极大元，即存在某 $I_0\in\mathcal{F}$ 使得不存在满足 $I_0\subsetneq J$ 的 $J\in\mathcal{F}$.

(iii)R 中每一个理想是有限生成的.

证明 (i)⇒(ii)：设 $\mathcal{F}$ 是 R 中的一些理想构成的一个集合，假设 $\mathcal{F}$ 无极大元. 取 $I_1\in\mathcal{F}$，因为 I_1 不是极大元，故存在 $I_2\in\mathcal{F}$ 使得 $I_1\subsetneq I_2$. 又 I_2 不是 $\mathcal{F}$ 中的极大元，故存在 I_3 使得 $I_2\subsetneq I_3$. 按这种方式继续下去，我们就可以得到 R 中的一个上升的理想链，且不停止，这与 R 满足 ACC 的假设矛盾.

(ii)⇒(iii)：设 I 是 R 中的一个理想，定义 $\mathcal{F}$ 为所有包含于 I 中且是有限生成的理想的全体. 当然 $\mathcal{F}\neq\varnothing$. 由假设，$\mathcal{F}$ 存在极大元 M. 因为 $M\in\mathcal{F}$，故 $M\subseteq I$. 若 $M\subsetneq I$，则存在 $a\in I$ 使得 $a\notin M$. 下面的理想

$$J=\{m+ra : m\in M, r\in R\}\subseteq I$$

是有限生成的，故 $J\in\mathcal{F}$. 但 $M\subsetneq J$ 且 M 是极大元，因此 $M=I$，从而 I 是有限生成的.

(iii)⇒(i)：假设 R 中每一个理想都是有限生成的，令

$$I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$$

为 R 中的一个上升的理想链. 由引理 7.14(i)，$J=\bigcup_n I_n$ 是一个理想. 由假设，存在元素 $a_i\in J$ 使得 $J=(a_1,\ \cdots,\ a_q)$. 又对某 n_i 有 a_i 一定落在某个 I_{n_i} 中. 设 N 是这些 n_i 中的最大者，故对所有的 i 有 $I_{n_i}\subseteq I_N$，所以

$$J=(a_1,\cdots,a_q)\subseteq I_N\subseteq J.$$

从而有，若 $n\geqslant N$，则 $J=I_N\subseteq I_n\subseteq J$，故 $I_n=J$. 从而此链停止，即 R 满足 ACC. ■

我们现在来给满足上命题中三个等价条件中的任一个的交换环一个名称.

定义 一个交换环 R 称为是一个**诺特环**[㊀]若 R 中的每一个理想都是有限生成的. 536

推论 7.27 设 I 是诺特环 R 中的一个理想，则在 R 中存在包含 I 的极大理想 M. 特别地，每一个诺特环都有极大理想.[㊁]

㊀ 为纪念爱米·诺特而命此名，爱米·诺特(Emmy Noether，1882—1935)在 1921 年引入了链条件.

㊁ 若不假设 R 是诺特环，此结果也是成立的，但一般结果的证明要用到佐恩引理.

证明　令$\mathcal{F}$是R中所有包含I的真理想构成的集合. 因为$I\in\mathcal{F}$，故$\mathcal{F}\neq\varnothing$. 因为$R$是诺特环，故由极大条件可知，$\mathcal{F}$中存在极大元$M$. 我们仍需要证明$M$是$R$中的极大理想(也就是，$M$实际上是由$R$中所有真理想构成的这个更大的集合$\mathcal{F}'$中的极大元). 假设存在真理想$J$使得$M\subseteq J$，则$I\subseteq J$，故$J\in\mathcal{F}$. 由$M$的极大性即有$M=J$，故$M$是$R$中的一个极大理想. ■

注　佐恩引理与极大条件[命题7.26中的(ii)]相关.

定义　**偏序集**是一个带有关系$x\preceq y$的非空集合X且对所有x，y，$z\in X$，有

(i)**反身性**：$x\preceq x$；

(ii)**反对称性**：若$x\preceq y$且$y\preceq x$，则$x=y$；

(iii)**传递性**：若$x\preceq y$，$y\preceq z$，则$x\preceq z$.

我们来推广我们的以前(在一族理想中)的极大元素的定义. 偏序集X中的一个元素u称为一个**极大元**若不存在$x\in X$使得$u\preceq x$且$u\neq x$.

设A是一个集合，若定义$U\preceq V$表示$U\subseteq V$，其中U和V是A的子集，则A的所有子集构成的集合$\mathcal{P}(A)$是一个偏序集. A的所有真子集构成的集合$\mathcal{P}(A)^{\cdot}$也是一个偏序集(更一般地，偏序集的每一个非空子集也是一个偏序集). 另一个例子是实数集$\mathbb{R}$，$x\preceq y$表示$x\leqslant y$. 存在具有多个极大元的偏序集[如$\mathcal{P}(A)^{\cdot}$]，也存在无极大元的偏序集[如$\mathbb{R}$]. 若某偏序集上佐恩引理成立，则它可保证此偏序集至少有一个极大元.

一个偏序集X称为一个**链**若对每两个a，$b\in X$，有或者$a\preceq b$，或者$b\preceq a$(因为在一个链中，每两个元素都是可比较的，因此相对于更一般的偏序集，链有时称为全序集). 我们现在
537 叙述佐恩引理.

佐恩引理　设X是一个偏序集，且X中的每一个链C都有一个上界，即，存在$x_0\in X$使得$c\preceq x_0$，对每一个$c\in C$. 则X有极大元.

可以证明佐恩引理等价于**选择公理**. 选择公理是说，任意(有可能无限多)个非空集的笛卡儿积也是非空的.

在处理诺特环时，通常不需要佐恩引理，因为极大条件就可保证任何一个由一些理想构成的非空的集$\mathcal{F}$均存在极大元. ◀

下面给出从一个诺特环构造一个新的诺特环的一个方法.

推论7.28　若R是一个诺特环，J是R中的一个理想，则R/J也是一个诺特环.

证明　设A是R/I中的一个理想，由对应定理，存在R中一个理想J使得$J/I=A$. 因为R是诺特环，故J是有限生成的. 设$J=(b_1, \cdots, b_n)$，故$A=J/I$是由陪集b_1+I，…，b_n+I生成的，因此每一个理想A是有限生成的，从而R/I是一个诺特环. ■

在1890年，希尔伯特证明了著名的希尔伯特基定理，他证明了$\mathbb{C}[x_1, \cdots, x_n]$中每一个理想都是有限生成的. 像我们将看到的一样，这个证明是非构造性的，即它没有给出理想的生成元的直接表达式. 据报道，当同时代的最杰出的代数学家之一戈丹(P. Gordan)第一次看到希尔伯特的证明时，他说："这不是数学，而是神学". 另一方面，当戈丹在1899年发表希尔伯特定理的一个简化证明时说："我确信神学也有它的优点".

下面这个希尔伯特基定理的优美的证明归功于萨杰斯(H. Sarges).

引理 7.29 一个交换环 R 是一个诺特环当且仅当 R 中的每一系列元素 a_1，…，a_n，…，存在 $m\geqslant 1$ 和 r_1，…，$r_m\in R$ 使得 $a_{m+1}=r_1a_1+\cdots+r_ma_m$.

证明 假设 R 不是一个诺特环，a_1，…，a_n，…是 R 中的一系列元素. 若 $I_n=(a_1, \cdots, a_n)$，则存在一个理想的上升的链 $I_1\subseteq I_2\subseteq\cdots$. 由 ACC 的假设，存在 $m\geqslant 2$ 使得 $I_m=I_{m+1}$. 因此 $a_{m+1}\in I_{m+1}=I_m$，所以存在 $r_i\in R$ 使得 $a_{m+1}=r_1a_1+\cdots+r_ma_m$.

反之，假设 R 满足关于元素链的条件. 若 R 不是一个诺特环，则存在一个不停止的理想的上升的链 $I_1\subseteq I_2\subseteq\cdots$. 必要时去掉重复项，我们可以假设对所有的 n 有 $I_n\subsetneq I_{n+1}$. 对每一个 n，选择 $a_{n+1}\in I_{n+1}$使得 $a_{n+1}\notin I_n$. 由假设，存在 m 和 $r_i\in R$，对 $i\leqslant m$，使得 $a_{m+1}=\sum_{i\leqslant m}r_ia_i\in I_m$. 这个矛盾就推出 R 是一个诺特环. ■ 538

定理 7.30(希尔伯特基定理) 若 R 是一个交换的诺特环，则 $R[x]$也是诺特环.

证明 设 I 是$R[x]$中的一个非有限生成的理想. 当然，$I\neq\{0\}$. 定义 $f_0(x)$为 I 中一个次数最低的多项式，归纳地，定义 $f_{n+1}(x)$为 $I-(f_0, \cdots, f_n)$中一个次数最低的多项式. 注意对所有 $n\geqslant 0$，$f_n(x)$是存在的. 若 $I-(f_0, \cdots, f_n)$是空的，则 I 是有限生成的. 显然

$$\deg(f_0)\leqslant\deg(f_1)\leqslant\deg(f_2)\leqslant\cdots.$$

记 a_n 为 $f_n(x)$的首项系数. 因为 R 是一个诺特环，应用引理 7.29，存在 m 使得 $a_{m+1}\in(a_0, \cdots, a_m)$，即，$r_i\in R$ 使得 $a_{m+1}=r_0a_0+\cdots+r_ma_m$. 定义

$$f^*(x)=f_{m+1}(x)-\sum_{i=0}^{m}x^{d_{m+1}-d_i}r_if_i(x),$$

其中 $d_i=\deg(f_i)$. 注意 $f^*(x)\in I-(f_0(x), \cdots, f_m(x))$，否则 $f_{m+1}(x)\in(f_0(x), \cdots, f_m(x))$ 只须证明 $\deg(f^*)<\deg(f_{m+1})$，因为这样就与 $f_{m+1}(x)$是不在$(f_0, \cdots, f_m)$中的最低的次数的多项式矛盾. 若 $f_i(x)=a_ix^{d_i}+$次数更低的项，则

$$\begin{aligned}f^*(x)&=f_{m+1}(x)-\sum_{i=0}^{m}x^{d_{m+1}-d_i}r_if_i(x)\\&=(a_{m+1}x^{d_{m+1}}+\text{次数更低的项})-\sum_{i=0}^{m}x^{d_{m+1}-d_i}r_i(a_ix^{d_i}+\text{次数更低的项}).\end{aligned}$$

首项被抵消，因此 $\sum_{i=0}^{m}r_ia_ix^{d_{m+1}}=a_{m+1}x^{d_{m+1}}$. ■

推论 7.31 (i)若 k 是一个域，则 $k[x_1, \cdots, x_n]$是诺特环.

(ii)环$\mathbb{Z}[x_1, \cdots, x_n]$是一个诺特环.

(iii)对 $k[x_1, \cdots, x_n]$中的任何理想 I，其中 $k=\mathbb{Z}$ 或 k 为一个域，则商环 $k[x_1, \cdots, x_n]/I$ 是诺特环.

证明 对 $n\geqslant 1$ 用归纳法. 头两条的证明运用上定理即可. 而(iii)的证明由推论 7.28 可得. ■

已知若 R 是一个诺特环，则形式幂系列环 $R[[x]]$也是一个诺特环(见扎理斯基一撒穆尔(Zariski-Samuel)所著的《交换代数 II》(Commutative Algebra II)的第 138 页). 539

习题

H 7.29 判断对错并给出理由.

(i)每一个交换环是一个诺特环.

(ii)一个诺特整环的每一个子环也是一个诺特环.

(iii)若 X, Y 是非空集，则 $X\times Y$ 也是非空集.

(iv)每一个偏序集至少有极大元.

(v)若$\mathcal{F}$是$\mathbb{F}_2[x, y]$中的理想的一个非空集，则$\mathcal{F}$的极大元就$\mathbb{F}_2[x, y]$中的极大理想.

(vi)若 A 满足 ACC，$J_1\supseteq J_2\supseteq J_3\supseteq\cdots$是 R 中一个理想链，则存在 M 使得 $J_M=J_{M+1}=J_{M+2}=\cdots$.

(vii)若 k 是一个域，则 $k[[x]]$是一个诺特环.

(viii)若 R 是一个交换环，$\varphi: \mathbb{Z}[x, y]\to R$ 是一个同态，则 $\ker\varphi$ 是有限生成的.

7.30 设 m 是一个正整数，X 是它的所有(正)因子构成的集合. 试证，若定义 $a\leq b$ 表示 $a\mid b$，则 X 是一个偏序集.

7.31 试证例题 3.11 中的环$\mathcal{F}(\mathbb{R})$不是一个诺特环.

7.32 令

$$S^2=\{(a,b,c)\in\mathbb{R}^3: a^2+b^2+c^2=1\}$$

表示$\mathbb{R}^3$ 的单位球面. 再令

$$I=\{f(x,y,z)\in\mathbb{R}[x,y,z]: f(a,b,c)=0,\text{对所有的}(a,b,c)\in S^2\}.$$

试证在$\mathbb{R}[x, y, z]$中，I 是一个有限生成的理想.

7.33 若 R 和 S 是诺特环，试证它们的直和 $R\times S$ 也是诺特环.

7.34 设 R 是一个环，也是域 k 上的一个向量空间，则称 R 为一个 k-代数若

$$(\alpha u)v=\alpha(uv)=u(\alpha v),$$

对所有的 $\alpha\in k$ 和 u, $v\in R$. 试证每一个有限维 k-代数都是一个诺特环.

7.4 簇

在解析几何中，我们给出了方程的图像. 例如，函数 f: $\mathbb{R}\to\mathbb{R}$ 的图像就是一条曲线，此曲线是由平面上所有有序对$(a, f(a))$构成，即，f 是方程

$$g(x,y)=y-f(x)=0$$

的所有解$(a, b)\in\mathbb{R}^2$ 的一个集合. 有些方程的图像不是函数的曲线，我们也能画出. 例如，多项式

540 $$h(x,y)=x^2+y^2-1$$

的所有零点的集合就是单位圆. 人们也能够给出$\mathbb{R}^2$ 中两个变量的多个多项式的共公解的图像. 事实上，人们能够给出$\mathbb{R}^n$ 中的 n 个变量的多个多项式的共公解的图像.

记号 设 k 是一个域，k^n 表示所有有序 n 元组构成的集合

$$k^n=\{(a_1,\cdots,a_n): a_i\in k,\text{对所有的 } i\}.$$

多个变量的多项式环 $k[x_1, \cdots, x_n]$记为 $k[X]$，其中 X 是

$$X=(x_1,\cdots,x_n)$$

的简写. 特别地，$f(x_1, \cdots, x_n)\in k[x_1, \cdots, x_n]$可简写为 $f(X)\in k[X]$.

在下面，我们将多项式 $f(x_1, \cdots, x_n)\in k[x_1, \cdots, x_n]$视为 $k^n\to k$ 的 n 个变量的函数，下

面是准确的定义.

定义 多项式 $f(X)\in k[X]$按下面明显的方式确定了一个**多项式函数** $f^\flat: k^n\to k$：若 $f(x_1, \cdots, x_n)=\sum_{e_1,\cdots,e_n} b_{e_1,\cdots,e_n}x_1^{e_1}\cdots x_n^{e_n}$ 且 $(a_1, \cdots, a_n)\in k^n$，则

$$f^\flat: (a_1,\cdots,a_n)\mapsto f(a_1,\cdots,a_n)=\sum_{e_1,\cdots,e_n} b_{e_1,\cdots,e_n}a_1^{e_1}\cdots a_n^{e_n}.$$

下一个命题推广了推论 3.52，将其中的一个变量推广为多个变量.

命题 7.32 设 k 是一个无限域，$k[X]=k[x_1, \cdots, x_n]$. 若 $f(X)$，$g(X)\in k[X]$满足 $f^\flat=g^\flat$，则 $f(x_1, \cdots, x_n)=g(x_1, \cdots, x_n)$.

证明 对 $n\geqslant 1$ 用归纳法. 基础步骤是推论 3.52. 下面证明归纳步骤. 记

$$f(X,y)=\sum_i p_i(X)y^i,\quad g(X,y)=\sum_i q_i(X)y^i,$$

其中 X 表示$(x_1, \cdots, x_n)$，$y=x_{n+1}$. 若 $f^\flat=g^\flat$，则对每一个 $a\in k^n$ 和每一个 $\alpha\in k$，有 $f(a, \alpha)=g(a, \alpha)$. 对一个固定的 $a\in k^n$，定义 $F_a(y)=\sum_i p_i(a)y^i$ 及 $G_a(y)=\sum_i q_i(a)y^i$. 因为 $F_a(y)$ 和 $G_a(y)$ 都在 $k[y]$ 中，由基础步骤，对所有的 $a\in k^n$，$p_i(a)=q_i(a)$. 由归纳假设，$p_i(X)=q_i(X)$，对所有的 i. 因此

$$f(X,y)=\sum_i p_i(X)y^i=\sum_i q_i(X)y^i=g(X,y).$$ ■

作为上命题的一个推论，当 k 是无限域时，我们去掉记号 $f^\flat$并将多项式和它的多项式函数等同. 由习题 3.104，代数闭域都是无限的. 因此当 k 是代数闭域时，命题 7.32 可以被应用. 541

定义 若 $f(X)\in k[X]=k[x_1, \cdots, x_n]$且 $f(a)=0$，其中 $a\in k^n$，则称 a 为 $f(X)$的一个**零点**. [若 $f(x)$是一个变量 x 的多项式，则 $f(x)$的零点也称为 $f(x)$的一个根.]

命题 7.33 若 k 是一个代数闭域且 $f(X)\in k[X]$不是一个常量，则 $f(X)$在 k^n 中有一个零点.

证明 对 $n\geqslant 1$ 用归纳法，其中 $X=(x_1, \cdots, x_n)$. 基础步骤由假设立即可得，因为 $k^1=k$ 是代数闭的. 与在命题 7.32 的证明中一样，记

$$f(X,y)=\sum_i g_i(X)y^i.$$

对每一个 $a\in k^n$，定义 $f_a(y)=\sum_i g_i(a)y^i$. 若 $f(X,y)$ 无零点，则每个 $f_a(y)\in k[y]$ 无零点，由基础步骤，$f_a(y)$ 是一个非零的常量，对所有 $a\in k^n$. 因此对所有的 $i>0$ 和所有的 $a\in k^n$，$g_i(a)=0$. 因为代数闭域是无限的，故可应用命题 7.32，从而知 $g_i(X)=0$，对所有的 $i>0$. 这样 $f(X,y)=g_0(X)y^0=g_0(X)$. 由归纳假设，$g_0(X)$ 就是一个非零的常量，命题得证. ■

我们现在来考虑多项式的解集.

定义 若 $F\subseteq k[X]=k[x_1, \cdots, x_n]$是一个子集，那么由 F 所定义的**代数集**是

$$\mathrm{Var}(F)=\{a\in k^n: f(a)=0, \text{对每一个 } f(X)\in F\}.$$

因此 $\mathrm{Var}(F)$[⊖] 由是每一个 $f(X)\in F$ 的零点的 $a\in k^n$ 构成的.

⊖ 记号 Var(F)来自于 Variety(簇)，它是后面即将定义的一种特殊的代数集.

例 7.34 (i)下面是由两个方程定义的一个代数集.

$$\mathrm{Var}(x,y)=\{(a,b)\in k^2: x=0 \text{ 或 } y=0\},$$

因此

$$\mathrm{Var}(x,y)=x\text{-轴}\cup y\text{-轴}$$

542 更一般地，任意有限个代数集的并仍是一个代数集.

(ii)**n-球面** S^n 定义为

$$S^n=\left\{(x_1,\cdots,x_{n+1})\in k^{n+1}:\sum_{i=1}^{n+1}x_i^2=1\right\}.$$

更一般地，定义 k^n 中的**超曲面**为由 $k[X]$中的单个多项式的所有零点所确定的代数集.

(iii)设 A 是元素在 k 中的 $m\times n$ 的矩阵. 由 n 个未知量的 m 个方程的一个方程组

$$AX=B,$$

其中 B 是一个 $n\times 1$ 列矩阵. 定义一个代数集：$\mathrm{Var}(AX=B)$，它是 k^n 的一个子集. 当然，$AX=B$ 实际上是 n 个变量的 m 个线性方程组的一个缩写，且 $\mathrm{Var}(AX=B)$通常称为方程组 $AX=B$ 的**解集**，当此方程组是齐次的，即当 $B=0$ 时，$\mathrm{Var}(AX=0)$是 k^n 的一个子空间，称为此方程组的**解空间**. ◀

下一个结果表明，只要涉及到簇，人们就可以假设 $k[X]$的子集 F 就是 $k[X]$的理想.

命题 7.35 *设 k 是一个域.*

(i)若 $F\subseteq G\subseteq k[X]$，则 $\mathrm{Var}(G)\subseteq\mathrm{Var}(F)$.

(ii)若 $F\subseteq k[X]$且 $I=(F)$是由 F 生成的理想，则

$$\mathrm{Var}(F)=\mathrm{Var}(I).$$

(iii)每一个代数集可以由有限个方程来定义.

证明 (i)若 $a\in\mathrm{Var}(G)$，则对所有的 $g(X)\in G$ 有 $g(a)=0$. 因为 $F\subseteq G$，故特别地，对所有 $f(X)\in F$，有 $f(a)=0$.

(ii)因为 $F\subseteq(F)=I$，故由(i)有 $\mathrm{Var}(I)\subset\mathrm{Var}(F)$. 下证反包含成立. 令 $a\in\mathrm{Var}(F)$，故对每一个 $f(X)\in F$ 有 $f(a)=0$. 若 $g(X)\in I$，则 $g(X)=\sum_i r_if_i(X)$，其中 $r_i\in k$，$f_i(X)\in F$. 因此 $g(a)=\sum_i r_if_i(a)=0$，故 $a\in\mathrm{Var}(I)$.

(iii)若 I 是 $k[X]$中一个理想，则由希尔伯特基定理，I 是有限生成的，即存在一个有限子集 $F\subseteq I$ 使得 $\mathrm{Var}(I)=\mathrm{Var}(F)$. ■

由此可得，并不是 k^n 的每个子集都是一个代数集. 例如，设 $n=1$，则 $k[x]$是一个 PID. 因此，若 F 是 $k[x]$的一个子集，则存在某个 $f(x)\in k[x]$使得$(F)=(f(x))$，从而

543 $$\mathrm{Var}(F)=\mathrm{Var}((F))=\mathrm{Var}((f))=\mathrm{Var}(f).$$

但 $f(x)$只有有限个根，故 $\mathrm{Var}(F)$是有限的. 若 k 是代数闭的，则它是一个有无限域，所以 $k^1=k$的大部分子集都不是簇.

尽管我们想在平面上画出图像，但当 $k=\mathbb{R}$ 时存在一个很大的缺陷：一些多项式没有零点. 例如，$f(x)=x^2+1$ 就没有根，故 $\mathrm{Var}(x^2+1)=\varnothing$. 更一般地，$g(x_1,\cdots,x_n)=x_1{}^2+\cdots+x_n{}^2+$

1 在 $\mathbb{R}^n$ 中就没有零点，故 $\mathrm{Var}(g)=\varnothing$. 因为我们正在处理（未必线性的）多项式，很自然的假设是得到它们所有可能的零点. 对于一个变量的多项式，这就是说 k 是代数闭的. 根据命题 7.33，我们知道当 k 是代数闭域时，对每一个非常量的 $f(X)\in k[X]$，$\mathrm{Var}(f)\neq\varnothing$. 当然，在任意域上考虑代数集是一个有趣的问题，但是在尝试理解复杂的问题之前，考虑最简单的情形是更理智的. 另一方面，下面的初步结论中许多在任意域 k 中都是有效的. 因此，我们将在每一个命题中陈述一下所需要的假设，但读者应该认识到，最重要的情形是 k 为代数闭域情形.

下面是 Var 的一些初步性质.

命题 7.36 令 k 是一个域.

(i) $\mathrm{Var}(x_1, x_1-1)=\varnothing$ 且 $\mathrm{Var}(0)=k^n$，其中 0 是零多项式.

(ii) 设 I 和 J 是 $k[X]$ 中的理想，则

$$\mathrm{Var}(IJ)=\mathrm{Var}(I\cap J)=\mathrm{Var}(I)\cup\mathrm{Var}(J),$$

其中 $IJ=\left\{\sum_i f_i(X)g_i(X) : f_i(X)\in I \text{ 且 } g_i(X)\in J\right\}$.

(iii) 设 $\{I_\ell : \ell\in L\}$ 是 $k[X]$ 中的一族理想，则

$$\mathrm{Var}\left(\sum_\ell I_\ell\right)=\bigcap_\ell \mathrm{Var}(I_\ell),$$

其中 $\sum_\ell I_\ell$ 是所有满足 $r_{\ell_i}\in I_{\ell_i}$ 的形如 $r_{\ell_1}+\cdots+r_{\ell_q}$ 的有限和构成的集合.

证明 (i) 若 $a=(a_1, \cdots, a_n)\in\mathrm{Var}(x_1, x_1-1)$，则 $a_1=0$ 且 $a_1=1$. 很清楚，不存在这样的点 a，故 $\mathrm{Var}(x_1, x_1-1)=\varnothing$. 至于 $\mathrm{Var}(0)=k^n$ 是显然的，因为每一个点 a 都是零多项式的根.

(ii) 因为 $IJ\subseteq I\cap J$，从而 $\mathrm{Var}(IJ)\supseteq\mathrm{Var}(I\cap J)$. 因为 $IJ\subseteq I$，从而 $\mathrm{Var}(IJ)\supseteq\mathrm{Var}(I)$. 因此

$$\mathrm{Var}(IJ)\supseteq\mathrm{Var}(I\cap J)\supseteq\mathrm{Var}(I)\cup\mathrm{Var}(J).$$

为完成证明，只须证明 $\mathrm{Var}(IJ)\subseteq\mathrm{Var}(I)\cup\mathrm{Var}(J)$. 若 $a\notin\mathrm{Var}(I)\cup\mathrm{Var}(J)$，则存在 $f(X)\in I$ 和 $g(X)\in J$ 使得 $f(a)\neq 0$ 及 $g(a)\neq 0$. 但 $f(X)g(X)\in IJ$ 且 $(fg)(a)=f(a)g(a)\neq 0$，因为 $k[X]$ 是一个整环. 因此 $a\notin\mathrm{Var}(IJ)$，得证. [544]

(iii) 对每一个 ℓ，由包含关系 $I_\ell\subseteq\sum_\ell I_\ell$ 知 $\mathrm{Var}\left(\sum_\ell I_\ell\right)\subseteq\mathrm{Var}(I_\ell)$，故

$$\mathrm{Var}\left(\sum_\ell I_\ell\right)\subseteq\bigcap_\ell \mathrm{Var}(I_\ell).$$

下证反包含关系. 若 $g(X)\in\sum_\ell I_\ell$，则存在有限多个 ℓ 使得 $g(X)=\sum_\ell h_\ell f_\ell$，其中 $h_\ell\in k[X]$ 且 $f_\ell(X)\in I_\ell$. 因此，若 $a\in\bigcap_\ell\mathrm{Var}(I_\ell)$，则 $f_\ell(a)=0$，对所有的 ℓ. 所以 $g(a)=0$，亦即 $a\in\mathrm{Var}\left(\sum_\ell I_\ell\right)$. ■

定义 集合 X 上的一个**拓扑**就是 X 的一些子集构成的集合 $\mathcal{F}$，$\mathcal{F}$ 中的子集称为**闭集**⊖，且满足下列公理：

(i) $\varnothing\in\mathcal{F}$ 且 $X\in\mathcal{F}$；

⊖ 人们也可以通过指定拓扑的开集的方式来定义拓扑，开集是闭集的补.

(ii)若 F_1，$F_2\in\mathcal{F}$，则 $F_1\cup F_2\in\mathcal{F}$，即两个闭集的并还是闭的；

(iii)若 $\{F_\ell:\ell\in L\}\subseteq\mathcal{F}$，则 $\bigcap_\ell F_\ell\in\mathcal{F}$，即闭集的交还是闭的.

一个**拓扑空间**就是一个有序的对$(X,\mathcal{F})$，其中 X 是一个集合，$\mathcal{F}$是 X 上的一个拓扑.

命题 7.36 表明了所有代数集构成的集合是一个拓扑，它被称为**扎里斯基拓扑**. 扎里斯基拓扑在对 $k[X]$的更深一步的研究中非常有用. $\mathbb{R}$ 上的通常的拓扑有许多闭集. 例如，每一个闭区间是一个闭集. 相反地是，在$\mathbb{R}$ 上的扎里斯基拓扑中，每一个闭集(除$\mathbb{R}$ 之外)是有限的.

给定 $k[X]$中的一个理想 I，我们刚刚定义了它的代数集 $\mathrm{Var}(I)\subseteq k^n$. 我们现在反向来考虑：给定一个子集 $A\subseteq k^n$，我们指定 $k[X]$中的一个理想给它，特别地，我们给每一个代数集指定一个理想.

定义 设 $A\subseteq k^n$，定义它的**坐标环** $k[A]$为由所有多项式函数 $f:k^n\to k$ 的限制 $f\mid A$ 构成的，运算像点的运算一样的交换环.

由 $\mathrm{res}:k[X]\to k[A]$给出的 $f(X)\mapsto f|A$ 的映射是一个环同态且此限制映射的核是 $k[X]$中的一个理想.

定义 若 $A\subseteq k^n$，定义

$$\mathrm{Id}(A)=\{f(X)\in k[X]=k[x_1,\cdots,x_n]:f(a)=0,\text{对每一个 } a\in A\}.$$

545 希尔伯特基定理告诉我们 $\mathrm{Id}(A)$总是一个有限生成的理想.

命题 7.37 若 $A\subseteq k^n$，则存在一个同构

$$k[X]/\mathrm{Id}(A)\cong k[A].$$

证明 限制映射 $\mathrm{res}:k[X]\to k[A]$是一个核为 $\mathrm{Id}(A)$的满射，故由第一同构定理可知结论成立. 注意两个在 A 上相等的多项式一定在 $\mathrm{Id}(A)$的同一个陪集中. ■

尽管对 $k[X]$任意的子集 F，$\mathrm{Var}(F)$的定义都是有意义的，但 F 是一个理想的情形才是最有趣的. 类似地，尽管对 k^n 的任意一个子集 A，$\mathrm{Id}(A)$的定义都是有意义的，但 A 是一个代数集的情形才是最有趣的. 总之，代数集是由一些(多项式)方程的解构成的，这才是我们所关心的.

命题 7.38 令 k 是一个域.

(i)$\mathrm{Id}(\varnothing)=k[X]$且若 k 是代数闭的，则 $\mathrm{Id}(k^n)=\{0\}$.

(ii)若 $A\subseteq B$ 是 k^n 的子集，则 $\mathrm{Id}(B)\subseteq\mathrm{Id}(A)$.

(iii)若$\{A_\ell:\ell\in L\}$是 k^n 的一些子集构成的集合，则

$$\mathrm{Id}\Big(\bigcup_\ell A_\ell\Big)=\bigcap_\ell \mathrm{Id}(A_\ell).$$

证明 (i)对某子集 $A\subseteq k^n$，若 $f(X)\in\mathrm{Id}(A)$，则 $f(a)=0$，对所有的 $a\in A$. 因此，若 $f(X)\notin\mathrm{Id}(A)$，则存在 $a\in A$ 使得 $f(a)\neq0$. 特别地，若 $A=\varnothing$，则每一个 $f(X)\in k[X]$一定在 $\mathrm{Id}(\varnothing)$中，因为没有元素 $a\in\varnothing$. 因此 $\mathrm{id}(\varnothing)=k[X]$.

若 $f(X)\in\mathrm{Id}(k^n)$，则 $f(a)=0$，对所有 $a\in k^n$. 由命题 7.32 可知，$f(X)$是零多项式.

(ii)若 $f(X)\in\mathrm{Id}(B)$，则 $f(b)=0$，对所有的 $b\in B$. 特别地，对所有的 $a\in A$ 有 $f(a)=0$，因为 $A\subseteq B$，所以 $f(X)\in\mathrm{Id}(A)$.

(iii)因为 $A_\ell\subseteq\bigcup_\ell A_\ell$，故对所有的 ℓ，我们有 $\mathrm{Id}(A_\ell)\supseteq\mathrm{Id}\Big(\bigcup_\ell A_\ell\Big)$. 因此 $\bigcap_\ell\mathrm{Id}(A_\ell)\supseteq\mathrm{Id}$

$(\bigcup_\ell A_\ell)$. 下面证明反包含. 假设 $f(X)\in\bigcap_\ell \mathrm{Id}(A_\ell)$，即 $f(a_\ell)=0$，对所有的 ℓ 及所有的 $a_\ell\in A_\ell$. 若 $b\in\bigcup_\ell A_\ell$，则存在某个 ℓ 使得 $b\in A_\ell$. 因此 $f(b)=0$. 所以 $f(X)\in\mathrm{Id}(\bigcup_\ell A_\ell)$. ■

人们希望有一个关于 $\mathrm{Id}(A\cap B)$的公式. $\mathrm{Id}(A\cap B)=\mathrm{Id}(A)\cup\mathrm{Id}(B)$肯定是不正确的，因为两个理想的并几乎一定不是一个理想(见习题 7.38).

当 V 是一个代数集时，下面一个概念出自于刻画形如 $\mathrm{Id}(V)$的那些理想的特征中. 546

定义 设 I 是交换环 R 中的一个理想，则它的**根**，记为$\sqrt{I}$，是

$$\sqrt{I}=\{r\in R: r^m\in I,\text{对某整数 } m\geqslant 1\}.$$

一个理想 I 称是一个**根理想**[⊖]若

$$\sqrt{I}=I.$$

习题 7.36 要求证明$\sqrt{I}$也是一个理想. 易见 $I\subseteq\sqrt{I}$，故一个理想 I 是一个根理想当且仅当$\sqrt{I}\subseteq I$. 例如，每一个素理想 P 是一个根理想，因为若 $f^n\in P$，则 $f\in P$. 下面有一个不是根理想的一个例子. 设 $b\in k$，令 $I=((x-b)^2)$. 则 I 不是一个根理想，因为$(x-b)^2\in I$，而$(x-b)\notin I$.

定义 交换环 R 中的一个元素 a 称为是**幂零的**若存在某 $n\geqslant 1$ 使得 $a^n=0$.

I 是交换环 R 中的一个根理想当且仅当 R/I 没有幂零元(当然，我们的意思是，R/I 没有非零的幂零元).

下面是我们引入根理想的原因.

命题 7.39 若对某 $A\subseteq k^n$，其中 k 是一个域，理想 $I=\mathrm{Id}(A)$，则 I 是一个根理想. 因此坐标环 $k[A]$没有幂零元.

证明 因为 $I\subseteq\sqrt{I}$总是成立的. 故只须验证反包含成立. 由假设，对某 $A\subseteq k^n$ 有 $I=\mathrm{Id}(A)$. 因此，若 $f\in\sqrt{I}$，则 $f^m\in\mathrm{Id}(A)$，即 $f(a)^m=0$，对所有的 $a\in A$. 但 $f(a)^m$ 在域 k 中，故由 $f(a)^m=0$ 可推出 $f(a)=0$，即 $f\in\mathrm{Id}(A)=I$. ■

命题 7.40 (i)若 I 和 J 是理想，则$\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$.

(ii)若 I 和 J 是根理想，则 $I\cap J$ 也是一个根理想.

证明 (i)若 $f\in\sqrt{I\cap J}$，则对某 $m\geqslant 1$，$f^m\in I\cap J$. 因此 $f^m\in I$ 且 $f^m\in J$，所以 $f\in\sqrt{I}$且 $f\in\sqrt{J}$，即 $f\in\sqrt{I}\cap\sqrt{J}$.

下证反包含. 假设 $f\in\sqrt{I}\cap\sqrt{J}$，则 $f^m\in I$，$f^q\in J$. 不妨设 $m\geqslant q$，则 $f^m\in I\cap J$，即 $f\in\sqrt{I\cap J}$.

(ii)若 I 和 J 是根理想，则 $I=\sqrt{I}$且 $J=\sqrt{J}$，故

$$I\cap J\subseteq\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}=I\cap J.$$ ■ 547

我们现来证明希尔伯特零点定理：$\sqrt{I}=\mathrm{Id}(\mathrm{Var}(I))$，对每一个理想 $I\subseteq\mathbb{C}[X]$，即，多项式 $f(X)$在 $\mathrm{Var}(I)$上取零值当且仅当 $f^m\in I$ 对某 $m\geqslant 1$. 此定理对 $k[X]$中的理想都成立，其中

⊖ 这个术语是合适的，因为若 $r^m\in I$，则它的 m 次根 r 也在 I 中.

k 是一个代数闭域. 精明的读者可以将我们这里给出的 $k=\mathbb{C}$ 情形的证明改写为任意不可数代数闭域 k 上的证明. 然而，证明一般定理，例如对于可数的素域的代数闭包，需要新的思想.

引理 7.41 *设 k 是一个域，$\varphi: k[X]\to k$ 是一个固定 k 中元素的满环同态. 若 $J=\ker\varphi$，则 $\mathrm{Var}(J)\neq\varnothing$.*

证明 注意对每个 i 有 $x_i\in k[X]$. 设 $\varphi(x_i)=a_i\in k$ 且 $a=(a_1,\cdots,a_n)\in k^n$. 若 $f(X)=\sum_{e_1,\cdots,e_n} c_{e_1,\cdots,e_n}x_1^{e_1}\cdots x_n^{e_n}\in k[X]$，则

$$\varphi(f(X))=\sum_{e_1,\cdots,e_n} c_{e_1,\cdots,e_n}\pi(x_1)^{e_1}\cdots\varphi(x_n)^{e_n}=\sum_{e_1,\cdots,e_n} c_{e_1,\cdots,e_n}a_1^{e_1}\cdots a_n^{e_n}=f(a_1,\cdots,a_n).$$

因此 $\varphi(f(X))=f(a)=\varphi(f(a))$，因为 $f(a)\in k$ 且 φ 固定 k 中的每一个点. 由此可得对每一个 $f(X)$，$f(X)-f(a)\in J$. 若 $f(X)\in J$，则 $f(a)\in J$. 但 $f(a)\in k$，且因为 J 是一个真理想，所以它不含非零的常量. 因此 $f(a)=0$ 且 $a\in\mathrm{Var}(J)$. ■

定理 7.42(弱零点定理) *若 $f_1(X),\cdots,f_t(X)\in\mathbb{C}[X]$，则理想 $I=(f_1,\cdots,f_t)$ 是 $\mathbb{C}[X]$ 中的一个真理想当且仅当*

$$\mathrm{Var}(f_1,\cdots,f_t)\neq\varnothing.$$

证明 有一个方向是清楚的：若 $\mathrm{Var}(I)\neq\varnothing$，则 I 是一个真理想. 因为 $\mathrm{Var}(\mathbb{C}[X])=\varnothing$.

下面证明反方向. 假设 I 是一个真理想. 由推论 7.27，存在包含 I 的一个极大理想 M，从而 $K=\mathbb{C}[X]/M$ 是一个域. 显然地，自然映射 $\mathbb{C}[X]\to\mathbb{C}[X]/M=K$ 将 $\mathbb{C}$ 映到自身. 故 $K/\mathbb{C}$ 是一个扩域，因此 K 是一个 $\mathbb{C}$ 上的向量空间. 因为所有首一多项式构成它的一组基，所以 $\mathbb{C}[X]$ 有可数的维数. 从而 $\dim_{\mathbb{C}}(K)$ 是可数的(也有可能是有限的).

假设 K 是 $\mathbb{C}$ 的一个真扩张，即存在某 $t\in K$ 使得 $t\notin\mathbb{C}$. 因为 $\mathbb{C}$ 是代数闭的，所以 t 不能为 $\mathbb{C}$ 上的代数元，故它就是一个超越元. 考虑 K 的子集 B，

548 $$B=\{1/(t-c): c\in\mathbb{C}\}$$

(注意 $t-c\neq0$ 因为 $t\notin\mathbb{C}$). 集合 B 是不可数的，因为它的指标集是不可数集 $\mathbb{C}$. 我们有 B 在 $\mathbb{C}$ 上是线性无关的. 若是这样的话，则与 $\dim_{\mathbb{C}}(K)$ 是可数的这一事实矛盾. 若 B 是线性相关的，则存在非零的 $a_1,\cdots,a_r\in\mathbb{C}$ 使得 $\sum_{i=1}^{r}a_i/(t-c_i)=0$. 消掉分母，我们有 $\sum_i a_i(t-c_1)\cdots\widehat{(t-c_i)}\cdots(t-c_r)=0$(因子 $t-c_i$ 被消去了). 用此式子定义多项式 $h(x)\in\mathbb{C}[x]$：

$$h(x)=\sum_i a_i(x-c_1)\cdots\widehat{(x-c_i)}\cdots(x-c_r).$$

注意 $h(t)=0$，t 的超越性推出 $h(t)$ 是零多项式. 另一方面，$h(c_1)=a_1(c_1-c_2)\cdots(c_1-c_r)\neq0$，故 $h(t)$ 不是零多项式，矛盾. 我们得出结论 $K/\mathbb{C}$ 不是真扩张，即 $K=\mathbb{C}$. 自然映射 $\mathbb{C}[X]\to K=\mathbb{C}[X]/M=\mathbb{C}$ 满足引理 7.41 的条件，所以 $\mathrm{Var}(M)\neq\varnothing$. 但 $\mathrm{Var}(M)\subseteq\mathrm{Var}(I)$，故完成证明. ■

德文 Nullstellensatz 翻译过来意思是“零点轨迹定理”，这是从下面推论而得名的.

推论 7.43 *对 $\mathbb{C}[X]$ 中的每一个理想 I，存在 $a=(a_1,\cdots,a_n)\in\mathbb{C}^n$ 使得 $f(a)=0$，对所有的 $f\in I$.*

证明 选择 $\mathrm{Var}(I)$ 中的任意一个元素 a. ■

在 $\mathbb{C}[X]=\mathbb{C}[x]$ 和 $f(x)\in\mathbb{C}[x]$ 不是一个常量情形中，存在 $a\in\mathbb{C}$ 使得 $f(a)=0$，即 $f(x)$

是一个复根. 因此弱零点定理是代数基本定理在多变量情形下的一个推广.

在下面的希尔伯特零点定理的证明中，我们用了"若宾维基(Rabinowitch)技巧"，即将 n 个变量的一个多项式环嵌入到一个 $n+1$ 个变量的多项式环中.

定理 7.44(零点定理) 若 I 是$\mathbb{C}[X]$中的一个理想，则

$$\mathrm{Id}(\mathrm{Var}(I))=\sqrt{I}.$$

因此 f 在 $\mathrm{Var}(I)$上为零当且仅当存在某 $m\geq 1$ 使得 $f^m\in I$.

证明 包含关系 $\mathrm{Id}(\mathrm{Var}(I))\geqslant\sqrt{I}$是显然成立的，因为若 $f^m(a)=0$，对某 $m\geq 1$ 及所有的 $a\in\mathrm{Var}(I)$，那么由 $f(a)\in\mathbb{C}$ 知，对所有的 a 有 $f(a)=0$.

下面证明包含成立. 假设 $h\in\mathrm{Id}(\mathrm{Var}(I))$，其中 $I=(f_1,\cdots,f_t)$，即若对所有的 i 有 $f_i(a)=0$，其中 $a\in\mathbb{C}^n$，则 $h(a)=0$. 我们必须证明 h 的某次方幂在 I 中. 当然，我们可假设 h 不是零多项式. 我们来假定：

$$\mathbb{C}[x_1,\cdots,x_n]\subseteq\mathbb{C}[x_1,\cdots,x_n,y],$$ 549

即每一个 $f(x_1,\cdots,x_n)$视为一个不依赖于最后一个变量 y 的 $n+1$ 个变量的多项式. 我们断言$\mathbb{C}[x_1,\cdots,x_n,y]$中的多项式

$$f_1,\cdots,f_t,1-yh$$

没有共同的零点. 若$(a_1,\cdots,a_n,b)\in\mathbb{C}^{n+1}$是一个公共的零点，则 $a=(a_1,\cdots,a_n)\in\mathbb{C}^n$ 是 $f_1,\cdots,f_t$ 的公共的零点，故 $h(a)=0$. 但 $1-bh(a)=1\neq 0$. 应用弱零点定理即可得 $\mathbb{C}[x_1,\cdots,x_n,y]$中的理想$(f_1,\cdots,f_t,1-yh)$不是一个真理想. 因此存在 $g_1,\cdots,g_{t+1}\in\mathbb{C}[x_1,\cdots,x_n,y]$使得

$$1=f_1g_1+\cdots+f_tg_t+(1-yh)g_{t+1}.$$

作替换 $y=1/h$，则上面牵涉 g_{t+1}的最后一项消失了. 将多项式 $g_i(X,y)$更清晰地表示：

$$g_i(X,y)=\sum_{j=0}^{d_i}u_j(X)y^j,$$

[故 $g_i(X,h^{-1})=\sum_{j=0}^{d_i}u_j(X)h^{-j}$]，我们看到

$$h^{d_i}g_i(X,h^{-1})\in\mathbb{C}[X].$$

因此，若 $m=\max\{d_1,\cdots,d_t\}$，则

$$h^m=(h^mg_1)f_1+\cdots+(h^mg_t)f_t\in I.$$ ■

定理 7.45 $\mathbb{C}[x_1,\cdots,x_n]$中的每一个极大理想 M 的形式为

$$M=(x_1-a_1,\cdots,x_n-a_n),$$

其中 $a=(a_1,\cdots,a_n)\in\mathbb{C}^n$，所以存在$\mathbb{C}^n$ 和$\mathbb{C}[x_1,\cdots,x_n]$中的极大理想间的一个双射.

证明 因为 M 是一个真理想，所以由定理 7.42，我们有 $\mathrm{Var}(M)\neq\varnothing$，即存在 $a=(a_1,\cdots,a_n)\in k^n$ 使得 $f(a)=0$ 对所有 $f\in M$. 因为 $\mathrm{Var}(M)=\{b\in k^n: f(b)=0$ 对所有 $f\in M\}$，所以我们有$\{a\}\subseteq\mathrm{Var}(M)$，因此. 命题 7.35 给出

$$\mathrm{Id}(\mathrm{Var}(M))\subseteq\mathrm{Id}(\{a\}).$$

注意定理 7.44 给出 $\mathrm{Id}(\mathrm{Var}(M))=\sqrt{M}$. 但是对每一个素理想 P 有$\sqrt{P}=P$，我们有 $\mathrm{Id}(\mathrm{Var}(M))=$

M. 注意 $\mathrm{Id}(\{a\})$是一个真理想，因为它没有包含非零常数. 所以 M 的极大性给出了 $M=\mathrm{Id}(\{a\})$.
550 我们来计算 $\mathrm{Id}(\{a\})=\{f(X)\in\mathbb{C}[X]: f(a)=0\}$. 若对每一个 i 有 $f_i(x_1, \cdots, x_n)=x_i-a_i$, 则 $f_i(a)=0$ 且 $x_i-a_i\in\mathrm{Id}(\{a\})$. 因此$(x_1-a_1, \cdots, x_n-a_n)\subseteq\mathrm{Id}(\{a\})$. 但是由推论 7.10, $(x_1-a_1, \cdots, x_n-a_n)$是一个极大理想，所以

$$(x_1-a_1,\cdots,x_n-a_n)=\mathrm{Id}(\{a\})=M. \quad ■$$

希尔伯特是在 1893 年证明零点定理的. 任意代数闭域上的零点定理的原始证明是在二十世纪二十年代应用"消去定理"而得的(扎理斯基一撒穆尔所著的《交换代数》的第 164 页～167 页). 更少的计算的证明，牵涉到雅名布森(Jacobson)环，是大约在 1960 年由克鲁尔(W. Krull)和哥德曼(O. Goldman)分别独立获得的.

尽管我们称定理 7.42 为弱零点定理，实际上，零点定理(定理 7.44)和定理 7.45 是等价的(参见习题 7.43).

我们继续算子 Var 和 Id 的研究.

命题 7.46 设 k 是一个域.

(i)对每一个子集 $A\subseteq k^n$,

$$\mathrm{Var}(\mathrm{Id}(A))\supseteq A.$$

(ii)对每一个理想 $I\subseteq k[X]$,

$$\mathrm{Id}(\mathrm{Var}(I))\supseteq I.$$

(iii)若 V 是 k^n 的一个代数集，则 $\mathrm{Var}(\mathrm{Id}(V))=V$.

证明 (i)此结果几乎是定义的重复. 若 $a\in A$，则对所有的 $f(X)\in\mathrm{Id}(A)$, $f(a)=0$. 由 $\mathrm{Id}(A)$的定义，$f(X)\in\mathrm{Id}(A)$在 A 上为零. 故 $a\in\mathrm{Var}(\mathrm{Id}(A))$. 因此 $\mathrm{Var}(\mathrm{Id}(A))\supseteq A$.

(ii)同样，我们仅需要看看定义. 若 $f(X)\in I$，则对所有的 $a\in\mathrm{Var}(I)$, $f(a)=0$. 因此，$f(X)$肯定是在 $\mathrm{Var}(I)$上为零的多项式之一.

(iii)若 V 是一个簇，则 $V=\mathrm{Var}(J)$, J 是 $k[X]$中某个理想. 又由(i),

$$\mathrm{Var}(\mathrm{Id}(\mathrm{Var}(J)))\supseteq\mathrm{Var}(J),$$

同样，由(ii)知，$\mathrm{Id}(\mathrm{Var}(J))\supseteq J$，应用命题 7.35(i)，即得反包含

$$\mathrm{Var}(\mathrm{Id}(\mathrm{Var}(J)))\subseteq\mathrm{Var}(J).$$

551 因此，$\mathrm{Var}(\mathrm{Id}(\mathrm{Var}(J)))=\mathrm{Var}(J)$，即 $\mathrm{Var}(\mathrm{Id}(V))=V$. ■

推论 7.47 (i)若 V_1 和 V_2 是代数集且 $\mathrm{Id}(V_1)=\mathrm{Id}(V_2)$，则 $V_1=V_2$.

(ii)若 I_1 和 I_2 是根理想且 $\mathrm{Var}(I_1)=\mathrm{Var}(I_2)$，则 $I_1=I_2$.

证明 (i)若 $\mathrm{Id}(V_1)=\mathrm{Id}(V_2)$，则 $\mathrm{Var}(\mathrm{Id}(V_1))=\mathrm{Var}(\mathrm{Id}(V_2))$. 由命题 7.46(iii)，我们有 $V_1=V_2$.

(ii)若 $\mathrm{Var}(I_1)=\mathrm{Var}(I_2)$，则 $\mathrm{Id}(\mathrm{Var}(I_1))=\mathrm{Id}(\mathrm{Var}(I_2))$. 由零点定理，$\sqrt{I_1}=\sqrt{I_2}$. 因为由假设 I_1, I_2 均为根理想，所以我们有 $I_1=I_2$. ■

下面这个定理总结了这些讨论.

定理 7.48 函数 $V\mapsto\mathrm{Id}(V)$和 $I\mapsto\mathrm{Var}(I)$保逆包含序的双射

$$\{代数集 \subseteq \mathbb{C}^n\} \rightleftarrows \{根理想 \subseteq \mathbb{C}[x_1, \cdots, x_n]\}.$$

证明 由命题 7.46，我们有 $\mathrm{Var}(\mathrm{Id}(V))=V$，对每一个代数集 V，而由定理 7.44 和 $\mathrm{Id}(\mathrm{Var}(I))=\sqrt{I}$，对每一个理想 I. ■

一个代数集可以分解成更小的代数子集的并吗？

定义 称一个代数集 V 是**不可约的**若它不是两个真代数子集的并，即 $V \neq W' \cup W''$，其中 W' 和 W'' 均为是 V 的真子集的代数集. 一个**簇**[㊀]就是指不可约的代数集.

命题 7.49 k^n 中的每个代数集都是有限多个簇的并：

$$V = V_1 \cup V_2 \cup \cdots \cup V_m.$$

证明 称代数集 $W \subseteq k^n$ 是好的若它是不可约的或是有限多个簇的并，否则称 W 为坏的. 我们必须证明不存在坏的簇. 若 W 是坏的，则它不是不可约的，故 $W=W' \cup W''$，其中 W' 和 W'' 均为真的代数子集. 但好的代数集的并也是好的，故 W' 和 W'' 中至少有一个是坏的，不妨设 W' 为坏的，给它重新命名为 $W'=W_1$. 对 W_1 重复这样的过程，得到一个坏的代数子集 W_2. 由归纳法可得出存在一个严格下降的序列：

$$W \supsetneq W_1 \supsetneq \cdots \supsetneq W_n \supsetneq \cdots. \quad 552$$

因为算子 Id 翻转包含关系，即存在一个严格的上升的理想链：

$$\mathrm{Id}(W) \subsetneq \mathrm{Id}(W_1) \subsetneq \cdots \subsetneq \mathrm{Id}(W_n) \subsetneq \cdots$$

[由推论 7.47(i)知包含关系是严格的]，这就与希尔伯特基定理矛盾. 我们得出结论，每一个代数集是好的. ■

簇有一个良好的特征.

命题 7.50 k^n 中一个代数集 V 是一个簇当且仅当 $\mathrm{Id}(V)$ 是 $k[X]$ 中的一个素理想. 因此簇 V 的坐标环 $k[V]$ 是一个整环.

证明 假设 V 是一个簇. 只须证明若 $f_1(X)$，$f_2(X) \notin \mathrm{Id}(V)$，则 $f_1(X)f_2(X) \notin \mathrm{Id}(V)$. 对 $i=1$，2，定义

$$W_i = V \cap \mathrm{Var}(f_i(X)).$$

注意每个 W_i 都是 V 的一个代数子集，因为它是两个代数子集的交. 进一步，因为 $f_i(X) \notin \mathrm{Id}(V)$，所以存在某 $a_i \in V$ 使得 $f_i(a_i) \neq 0$，故 W_i 是 V 的一个真代数子集. 因为 V 是不可约的，所以我们不能有 $V=W_1 \cup W_2$. 因此存在某 $b \in V$ 且 b 不在 $W_1 \cup W_2$ 中. 也就是 $f_1(b) \neq 0 \neq f_2(b)$. 因此 $f_1(b)f_2(b) \neq 0$. 因此 $f_1(X)f_2(X) \notin \mathrm{Id}(V)$，所以 $\mathrm{Id}(V)$ 是一个素理想.

相反，假设 $\mathrm{Id}(V)$ 是一个素理想. 设 $V=V_1 \cup V_2$，其中 V_1 和 V_2 是代数子集. 若 $V_2 \subsetneq V$，则我们必须证明 $V=V_1$. 由

$$\mathrm{Id}(V) = \mathrm{Id}(V_1) \cap \mathrm{Id}(V_2) \supseteq \mathrm{Id}(V_1)\mathrm{Id}(V_2).$$

命题 7.38 给出上面的等式，习题 7.12 给出上面的不等式. 因为 $\mathrm{Id}(V)$ 是一个素理想，习题 7.12(ii)表明 $\mathrm{Id}(V_1) \subseteq \mathrm{Id}(V)$ 或 $\mathrm{Id}(V_2) \subseteq \mathrm{Id}(V)$. 但 $V_2 \subsetneq V$ 可推出 $\mathrm{Id}(V_2) \supsetneq \mathrm{Id}(V)$. 故我

㊀ 术语 variety(簇)是由贝尔特拉米(E. Beltami，受高斯启发)将黎曼(Riemann)用的德文术语 Mannigfaltigkeit 翻译而得. 当今术语 Mannigfaltigkeit 通常译成 manifold(流形).

们得出结论 $\mathrm{Id}(V_1)\subseteq\mathrm{Id}(V)$. 但逆不等式 $\mathrm{Id}(V_1)\supseteq\mathrm{Id}(V)$ 一样成立，因为 $V_1\subseteq V$，故 $\mathrm{Id}(V_1)=\mathrm{Id}(V)$. 因此由推论 7.47 有 $V_1=V$，所以 V 是不可约的，即 V 是一个簇. ■

我们考虑在一个代数集的簇的分解中，这些簇是否是唯一确定的. 有一个明显的方式得到非唯一性. 假设存在 $k[X]$中的两个素理想 $P\subsetneq Q$.（例如$(x)\subsetneq(x, y)$就是 $k[x, y]$中的这样的理想）. 由于 $\mathrm{Var}(Q)\subsetneq\mathrm{Var}(P)$，故若 $\mathrm{Var}(P)$是簇 V 的一个子簇，如设 $V=\mathrm{Var}(P)\cup V_2\cup\cdots\cup V_m$，则 $\mathrm{Var}(Q)$可以是 V_i 中的某一个或被去掉.

定义 称一个分解 $V=V_1\cup\cdots\cup V_m$ 是**不冗长的并**，若没有一个 V_i 可以被删去，即对所有的 i，

553 $$V\neq V_1\cup\cdots\cup\hat{V}_i\cup\cdots\cup V_m.$$

命题 7.51 每一个代数集 V 是簇的一个不冗长的并

$$V=V_1\cup\cdots\cup V_m.$$

进一步，这些簇 V_i 是由 V 唯一确定的.

证明 由命题 7.49，V 是有限多个簇的并，不妨设 $V=V_1\cup\cdots\cup V_m$. 若选择 m 为使上式成立的最小者，则此并就是不冗长的.

我们现在来证明唯一性. 假设 $V=W_1\cup\cdots\cup W_s$ 是簇的一个不冗长的并. 令 $X=\{V_1, \cdots, V_m\}$，$Y=\{W_1, \cdots, W_s\}$. 我们将证明 $X=Y$. 若 $V_i\in X$，我们有

$$V_i=V_i\cap V=\bigcup_j(V_i\cap W_j).$$

注意对某 j 有 $V_i=V_i\cap W_j\neq\varnothing$. 因为 V_i 是不可约的，所以存在唯一的这样的 W_j. 因此 $V_i=V_i\cap W_j$，故 $V_i\subseteq W_i$. 对 W_j 用同样的论断可证明，确实地存在一个 V_ℓ 使得 $W_j\subset V_\ell$. 因此

$$V_i\subseteq W_j\subseteq V_\ell.$$

因为并 $V_1\cup\cdots\cup V_m$ 是不冗长的，所以我们一定有 $V_i=V_\ell$，故 $V_i=W_j=V_\ell$，即 $V_i\in Y$ 及 $X\subseteq Y$. 同理可证明反包含成立. ■

定义 交 $I=J_1\cap\cdots\cap J_m$ 是一个**不冗长的交**若没有 J_i 可以被删去，即对所有的 i，

$$I\neq J_1\cap\cdots\cap\hat{J}_i\cap\cdots\cap J_m.$$

推论 7.52 $k[X]$中每一个根理想 J 是素理想的一个不冗长的交，

$$J=P_1\cap\cdots\cap P_m.$$

进一步，素理想 P_i 是被 J 唯一确定的.

证明 因为 J 是一个根理想，所以存在一个簇 V 使得 $J=\mathrm{Id}(V)$. 由 V 是不可约子簇的一个不冗长的并，

$$V=V_1\cup\cdots\cup V_m,$$

故

554 $$J=\mathrm{Id}(V)=\mathrm{Id}(V_1)\cap\cdots\cap\mathrm{Id}(V_m).$$

由命题 7.50，V_i 是不可约的可推出 $\mathrm{Id}(V_i)$是素的，所以 J 是素理想的交，这是一个不冗长的交，因为若存在 ℓ 使得 $J=\mathrm{Id}(V)=\bigcap_{j\neq\ell}\mathrm{Id}(V_j)$，则

$$V = \mathrm{Var}(\mathrm{Id}(V)) = \bigcup_{j\neq \ell} \mathrm{Var}(\mathrm{Id}(V_j)) = \bigcup_{j\neq \ell} V_j,$$

与并是不冗长的假设相矛盾.

类似也可证明唯一性. 若 $J=\mathrm{Id}(W_1)\cap\cdots\cap\mathrm{Id}(W_s)$，其中每一个 $\mathrm{Id}(W_i)$是一个素理想(因此是一个根理想)，则每一个 W_i 是一个不可约的簇. 用 Var 作用将 $V=\mathrm{Var}(\mathrm{Id}(V))=\mathrm{Var}(J)$ 表示为不可约的子簇的不冗长的并. 由此分解的唯一性可得出交中素理想的唯一性. ■

当人们进一步考查这些思想时，有些自然的问题产生了. 首先，一个簇的维数是什么? 存在不同的候选，结果表明素理想是关键所在. 若 V 是一个簇，则它的维数就是它的坐标环 $k[V]$中的最长的素理想链的长度(由对应定理，维数也是 $k[X]$中在 $\mathrm{Id}(V)$之上的最长的素理想链的长度). 另一个问题牵涉到交. 若 $\mathrm{Var}(f)$是由一个次数为 d 的多项式而得的一个曲面，则有多少点在 V 与一条直线的交中? 伯祖特(Bézout)定理说，应该存在 d 个根. 但我们应该注意，首先必须要求系数域是代数闭的，以免 $\mathrm{Var}(f)=\varnothing$ 出现问题. 但也许有重根，故为使得伯祖特定理成立，一些交不得不算成带有一定的重数，为高维簇的交定义维数是十分巧妙的工作.

事实表明在一个大的**射影空间**中讨论会更方便一些. 回忆到我们给出了域 k 上的射影空间的两种构造. 在第 3.9 节中，我们通过添加一条无穷远处的直线至平面 k^2 上构造了一个射影空间，此方法可以推广至高维：添加了一个"无穷远处的超平面"至 k^n 上. 为将子集 k^n 与射影空间区分开来，人们称 k^n 为**仿射空间**，因为它由"有限点"构成—也就是，没有点在无穷远处. 在例 4.26 中，我们给出了射影空间的另一个构造，它的点实际上是 k^3 中通过原点的直线. 此构造中的每一个点有**齐次坐标**$[a_0, a_1, a_2]$，其中 $a_i\in k$ 且若存在一个非零的 $t\in k$ 使得 $a_i'=ta_i$，对所有的 i，则$[a_0', a_1', a_2']=[a_0, a_1, a_2]$. 对固定的 $n\geq 1$，在 $k^{n+1}-\{0\}$上定义一个等价关系为

$$(a_0',\cdots,a_n') \equiv (a_0,\cdots,a_n)$$

若存在一个非零的 $t\in k$ 使得 $a_i'=ta_i$，对所有的 i. 记$(a_0, \cdots, a_n)$所在的等价类为$[a_0, \cdots, a_n]$，称之为一个**射影点**，定义 k 上的**射影 n-空间**为所有射影点构成的集合，记为$\mathbb{P}_n(k)$. 现在很自然地，定义射影代数集为一组多项式的零点. 例如，若 $f(X)\in k[X]=k[x_0, x_1, \cdots, x_n]$，则定义 555

$$\mathrm{Var}(f) = \{[a_0,\cdots,a_n] \in \mathbb{P}_n(k) : f([a_0,\cdots,a_n]) = 0\}.$$

此定义有一个问题：$f(X)$是定义在 k^{n+1}中的点上，而不是射影点上的，也就是，我们需要 $f(a_0, \cdots, a_n)=0$ 当且仅当 $f(ta_0, \cdots, ta_n)=0$，其中 t 是非零的. 一个多项式 $f(x_0, \cdots, x_n)$称为 **$m>0$ 次齐次的**若

$$f(tx_0,\cdots,tx_n) = t^m f(x_0,\cdots,x_n)$$

对所有的 $t\in k$. 例如，单项式 $cx_0^{e_0}\cdots x_n^{e_n}$ 是一个 m 次齐次的，其中 $m=e_0+\cdots+e_n$ 是它的全次数，一个多项式 $f(X)\in k[X]$是 m 次齐次的若 $f(X)=\sum c_{e_0,\cdots,e_n} x_0^{e_0}\cdots x_n^{e_n}$，其中单项式的全次数全部为 m. 若 $f(X)$是齐次的且 $f(a_0, \cdots, a_n)=0$，则 $f(ta_0, \cdots, ta_n)=t^m f(a_0, \cdots, a_n)=0$. 因此当 $f(X)$是齐次的多项式时，我们称一个射影点为 f 的一个零点是有意义的. 定义射影

代数集如下

定义 若 $F\subseteq k[X]=k[x_0, \cdots, x_n]$ 是一组齐次的多项式，则由 F 定义的**射影代数集**为

$$\mathrm{Var}(F) = \{[a] \in \mathbb{P}_n(k) : f([a]) = 0, \text{对每一个 } f(X) \in F\},$$

其中 $[a]$ 是 $[a_0, \cdots, a_n]$ 的简记形式.

引入射影空间的原因是经常出现这样的情况：许多分离的仿射情形变成了一个更简单的射影情形的一部分. 事实上，伯祖特定理就是这种现象的一个例子.

习题

H 7.35 试证交换环 R 中的一个元素 a 是幂零的当且仅当 $1+a$ 是一个单位.

*H 7.36 设 I 是交换环 R 中的一个理想，试证它的根 $\sqrt{I}$ 也是一个理想.

7.37 设 R 是一个交换环，则它的**幂零根** $\mathrm{nil}(R)$ 定义为 R 中所有素理想的交. 试证 $\mathrm{nil}(R)$ 就是 R 中所有幂零元构成的集合：

$$\mathrm{nil}(R) = \{r \in R : r^m = 0, \text{对某 } m \geqslant 1\}.$$

*7.38 若 I 和 J 是 $\mathbb{C}[X]$ 中的理想，试证 $\mathrm{Id}(\mathrm{Var}(I) \cap \mathrm{Var}(J)) = \sqrt{I+J}$.

7.39 若 k 是一域，k^n 的形如 $\mathrm{Var}(f)$ 的子集称为一个超曲面，其中 $f\in k[x_1, \cdots, x_n]$. 试证每一个代数集 $\mathrm{Var}(I)$ 是有限多个超曲面的交.

7.40 (i) 试证 x^2+y^2 在 $\mathbb{R}[x, y]$ 中是不可约的，由此得出 (x^2+y^2) 是 $\mathbb{R}[x, y]$ 中的一个素理想，从而是一个根理想.

556 (ii) 试证 $\mathrm{Var}(x^2+y^2)=\{(0, 0)\}$.

(iii) 试证 $\mathrm{Id}(\mathrm{Var}(x^2+y^2)) > (x^2+y^2)$，由此得出在 $\mathbb{R}[x, y]$ 中，根理想 (x^2+y^2) 不能表成形式 $\mathrm{Id}(V)$，这里 V 是某个代数集. 从而得出结论，若 k 不是代数闭的，则零点定理可能不成立.

(iv) 试证在 $\mathbb{C}[x, y]$ 中，$(x^2+y^2)=(x+\mathrm{i}y)\cap(x-\mathrm{i}y)$.

(v) 试证在 $\mathbb{C}[x, y]$ 中，$\mathrm{Id}(\mathrm{Var}(x^2+y^2))=(x^2+y^2)$.

7.41 试证 $\mathbb{C}[X]$ 中的每个根理想是一些素理想的不冗长的交.

7.42 试证，$f_1, \cdots, f_t\in \mathbb{C}[X]$，则 $\mathrm{Var}(f_1, \cdots, f_t)=\varnothing$ 当且仅当存在 $h_1, \cdots, h_t\in k[X]$ 使得

$$1 = \sum_{i=1}^{t} h_i(X) f_i(X).$$

*7.43 考虑下面的论断.

Ⅰ. 若 I 是 $\mathbb{C}[X]$ 中的一个真理想，则 $\mathrm{Var}(I)\neq\varnothing$.

Ⅱ. $\mathrm{Id}(\mathrm{Var}(I))=\sqrt{I}$.

Ⅲ. $\mathbb{C}[X]$ 中的每一个极大理想形如 $(x_1-a_1, \cdots, x_n-a_n)$.

证明 Ⅲ⇒Ⅰ.（我们已经证明了Ⅰ⇒Ⅱ和Ⅱ⇒Ⅲ）

7.44 设 R 是一个交换环，设

$$\mathrm{Spec}(R)$$

表示 R 中的所有素理想构成的集合. 若 $E\subseteq\mathrm{Spec}(R)$，定义 $\mathrm{Spec}(R)$ 的子集 $E=\{P_\alpha : \alpha\in A\}$ 的闭包为

$$\overline{E} = \{\text{所有满足 } P_\alpha \subseteq P \text{ 的素理想 } P \in R, \text{对所有的 } P_\alpha \in E\}.$$

试证：(i) $\overline{\{0\}}=\mathrm{Spec}(R)$.

(ii) $\overline{R}=\varnothing$.

(iii) $\overline{\sum_{\ell} E_{\ell}} = \bigcap_{\ell} \overline{E_{\ell}}$.

(iv) $\overline{E \cap F} = \overline{E} \cup \overline{F}$.

由此得出结论，Spec(R)中所有形如 $\overline{E}$ 子集构成的集合是 Spec(R)上的一个拓扑. 此拓扑称为**扎里斯基拓扑**.

7.45 试证在 Spec(R)中，一个理想 P 是闭的当且仅当 P 是一个极大理想.

7.46 若 X 和 Y 是拓扑空间，则称函数 $g: X \to Y$ 是**连续的**若对 Y 的每一个闭集 Q，逆象 $g^{-1}(Q)$是 X 的一个闭集. 设 $f: R \to A$ 为一个环同态，定义 $f^{*}: \mathrm{Spec}(A) \to \mathrm{Spec}(R)$为 $f^{*}(Q) = f^{-1}(Q)$，其中 Q 是 A 中任一个素理想. 试证，f^{*} 是一个连续函数.

7.47 试证由

$$\varphi: (a_1, \cdots, a_n) \mapsto (x_1 - a_1, \cdots, x_1 - a_n),$$

定义的函数 $\varphi: \mathbb{C}^n \to \mathrm{Spec}(\mathbb{C}[x_1, \cdots, x_n])$是一个单的连续函数(这里$\mathbb{C}^n$ 和 $\mathrm{Spec}(\mathbb{C}[x_1, \cdots, x_n])$都带有扎里斯基拓扑，$\mathbb{C}^n$ 上的扎里斯基拓扑如前面定义. 557

7.48 试证明$\mathbb{C}^n$ 中的闭集构成的下降链

$$F_1 \supseteq F_2 \supseteq \cdots \supseteq F_m \supseteq F_{m+1} \supseteq \cdots$$

会停止：存在某 t 使得 $F_t = F_{t+1} = \cdots$.

7.5 广义的除法算式

给定两个多项式 $f(x)$，$g(x) \in k[x]$，这里 $g(x) \neq 0$，k 是一个域，何时 $g(x)$是 $f(x)$的一个因式？除法算式指出，存在唯一的多项式 $q(x)$，$r(x) \in k[x]$，使得

$$f(x) = q(x)g(x) + r(x),$$

这里 $r=0$ 或 $\deg(r) < \deg(g)$. 故 $g \mid f$ 当且仅当余式 $r=0$. 让我们从另一个角度来看这个公式：$g \mid f$ 就意味着 $f \in (g)$，由 $g(x)$生成的主理想. 因此，余式 r 是 f 在此理想中的障碍，也就是 $f \in (g)$当且仅当 $r=0$.

考虑更一般的问题. 给定多项式

$$f(x), g_1(x), \cdots, g_m(x) \in k[x],$$

其中 k 是一个域，什么时候 $d(x) = \gcd\{g_1(x), \cdots, g_m(x)\}$是 f 的一个因式？欧氏算法可求出 d，除法算式决定是否有 $d \mid f$. 从另一个角度上看，这两个经典的算法结合在一块就给出了一个判定是否有 $f \in (g_1, \cdots, g_m) = (d)$的算法.

给定 $f(X)$，$g_1(X)$，…，$g_m(X) \in k[X]$，我们现在问是否存在 $k[x_1, \cdots, x_n] = k[X]$中的一个能够判断是否有 $f \in (g_1, \cdots, g_m)$算法？$k[X]$中的除法算式将是一个产生

$$r(X), a_1(X), \cdots, a_m(X) \in k[X]$$

使得

$$f = a_1 g_1 + \cdots + a_m g_m + r,$$

其中 $r(X)$唯一，的一个算法. 因为$(g_1, \cdots, g_m)$由这些 g_i 的所有线性组合构成，所以这样的一个广义的算律将再一次表明余式 r 是一个阻碍：$f \in (g_1, \cdots, g_m)$当且仅当 $r=0$.

我们现在来证明除法算式和欧氏算法都可推广至多变量的多项式. 尽管这些结论是初等

的，但它们是最近（1965 年）由布切贝哥（B. Buchberger）发现．代数总是处理算律，但是自 19 世纪后半叶凯莱（Cayley）和戴德金（Dedekind）之后，公理化的方法的作用及美丽主宰了这
558 门学科．在 1948 年交换机发现之后，高速计算变成了一个现实，旧的复杂的算法以及一些新的算法都可以实施，更高阶的计算进入了代数．经典算法由单变量的多项式到多变量的多项式的推广正在被发现，计算机科学的发展极有可能是一个主要原因．这也是外部思想对数学的影响的一个戏剧性的解释．

7.5.1 单项式序

$k[x]$中的除法算式的最重要的特征是余式 $r(x)$ 具有小的次数．若没有不等式 $\deg(r)<\deg(g)$，此结论实质上是无用的，因为对给定的任一个 $Q(x)\in k[x]$，总有等式

$$f(x)=Q(x)g(x)+[f(x)-Q(x)g(x)].$$

多个变量的多项式是形如 $cx_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 的单项式的和，其中 $c\in k$，且对所有的 i 有 $\alpha_i\geqslant 0$．下面是单项式次数的两个规定．

定义 一个单项式 $cx_1^{\alpha_1}\cdots x_n^{\alpha_n}\in k[x_1,\cdots,x_n]$的**多重次数**是有序 n 元数组 $\alpha=(\alpha_1,\cdots,\alpha_n)$，其中 $c\in k$ 是非零的且对所有 i 有 $\alpha_i\geqslant 0$．它的**总次数**是和 $|\alpha|=\alpha_1+\cdots+\alpha_n$．

在 $k[X]$中，当用 $g(x)$去除 $f(x)$时，人们通常是根据次数将 $f(x)$的单项用下降的顺序来排列的：

$$f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_2x^2+c_1x+c_0,$$

考虑多变量的多项式：

$$f(X)=f(x_1,\cdots,x_n)=\sum c_{(\alpha_1,\cdots,\alpha_n)}x_1^{\alpha_1}\cdots x_n^{\alpha_n}.$$

我们将$(\alpha_1,\cdots,\alpha_n)$简记为 α，$x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 简记为 X^α，故 $f(X)$可更紧凑地写成

$$f(X)=\sum_\alpha c_\alpha X^\alpha.$$

我们的目标是将 $f(X)$中所有的单项式按一种合理的方式来排列，我们通过对它们的多重次数排序来完成这些工作．

由自然数的所有有序的 n 元数组构成的集合$\mathbb{N}^n$ 关于下加法是一个幺半群[⊖]：

559 $$(\alpha_1,\cdots,\alpha_n)+(\beta_1,\cdots,\beta_n)=(\alpha_1+\beta_1,\cdots,\alpha_n+\beta_n).$$

此幺半群的运算是与单项式的乘法相关的：

$$X^\alpha X^\beta=X^{\alpha+\beta}.$$

回忆到，一个偏序集是一个带有关系$\preceq$的非空集合，这里关系$\preceq$满足反身性，反对称性和传递性．当然，我们可记为 $x\prec y$ 若 $x\preceq y$ 且 $x\neq y$．我们也可用 $y\succeq x$（或 $y\succ x$）来代替 $x\preceq y$（或 $x\prec y$）．

定义 一个偏序集 X 称为是**良序的**若每一个非空集 $S\subseteq X$ 包含一个最小元，也就是，存在 $s_0\in S$ 使得对所有 $s\in S$ 有 $s_0\preceq s$．

⊖ 回忆到幺半群是一个带有一个满足结合律的运算且有单位元的集合．在这里，运算是＋，单位元是(0，…，0)且运算满足交换律：$\alpha+\beta=\beta+\alpha$．

例如，最小整数公理说，带有通常不等关系$\leqslant$，的自然数集N是良序的.

命题 7.53 设 X 是一个良序集.

(i)若 x，$y\in X$，则 $x\preceq y$ 或 $y\preceq x$.

(ii)每一个严格递减的序列是有限的.

证明 (i)子集 $S=\{x, y\}$ 有一个最小元，一定为 x 或 y. 在第一种情形下，$x\preceq y$；在第二种情形下，$y\preceq x$.

(ii)假设存在一个无限严格递减的序列，如

$$x_1 \succ x_2 \succ x_3 \succ \cdots.$$

因为 X 是良序的，故由所有 x_i 构成的子集 S 有最小元素，设为 x_n，但 $x_{n+1}\prec x_n$，矛盾！ ■

良序集的第二个性质将会用于证明一个算法最终会停止. 例如，在一个变量的多项式的除法算式的证明中，我们对每一步都连接一个自然数：余式项的次数. 进一步，若算律在一个给定的步骤处没有停止，则连接下一步的自然数，即它的余式项的次数，此数是严格变小的. 因为按通常的不等关系$\leqslant$，自然数集是良序的，故这个自然数的严格递减序列一定是有限的，也就是说，此算律在有限步后一定停止.

我们对多重次数的排序感兴趣，多重次数与幺半群$\mathbb{N}^n$ 中的乘法，即加法，是相容的.

定义 **单项式序**是$\mathbb{N}^n$ 的一个良序，且满足

$$\alpha\preceq\beta \text{ 可推出 } \alpha+\gamma\preceq\beta+\gamma,$$

对所有的 α，β，$\gamma\in\mathbb{N}^n$.

$\mathbb{N}^n$ 上的一个单项式序给出了 $k[X]=k[x_1, \cdots, x_n]$中的单项式的一个排序：当 $\alpha\preceq\beta$ 时，我们就定义 $X^\alpha\preceq X^\beta$，即单项式将根据它们的多重次数来排序. 560

定义 设$\mathbb{N}^n$ 带有一个单项式序，则每一个 $f(X)\in k[X]=k[x_1, \cdots, x_n]$按项的次数下降的方式可写成：首先是它的最高次项，接着是它的其他的次数更低的项，$f(X)=c_\alpha X^\alpha+$低次项. 定义它的**首项**为

$$\mathrm{LT}(f) = c_\alpha X^\alpha,$$

它的**次数**为

$$\mathrm{DEG}(f) = \alpha.$$

称 $f(X)$为**首一的**若 $\mathrm{LT}(f)=X^\alpha$，即若 $c_\alpha=1$.

存在许多种单项式序的定义，但我们只给出下两种最通用的.

定义 $\mathbb{N}^n$ 上的**字典序**定义为 $\alpha\preceq_{\mathrm{lex}}\beta$ 当 $\alpha=\beta$ 或 $\beta-\alpha$ 的第一个非零的坐标是正的[⊖].

术语字典序来自于在字典中的标准顺序. 若 $\alpha\prec_{\mathrm{lex}}\beta$，则它们在开始的 $i-1$ 个坐标上相等(这里 $i\geqslant1$)，即 $\alpha_1=\beta_1$，$\cdots$，$\alpha_{i-1}=\beta_{i-1}$，并有严格不等式：$\alpha_i<\beta_i$. 例如按字典序下列德文单词是增加的(字母排序为 $a<b<c<\cdots<z$)：

ausgehen

ausladen

auslagen

⊖ 差 $\beta-\alpha$ 可能不在$\mathbb{N}^n$ 中，但一定在$\mathbb{Z}^n$ 中.

auslegen

bedeuten

命题 7.54 N^n 上的字典序$\leq_{lex}$是一个单项式序.

证明 首先我们证明字典序是一个偏序. 关系$\leq_{lex}$是反身的，因它的定义表明 $\alpha\leq_{lex}\alpha$. 下面证明反对称性，假设 $\alpha\leq_{lex}\beta$ 且 $\beta\leq_{lex}\alpha$. 若 $\alpha\neq\beta$，则它们的坐标中有不等的，设第一个为第 i 个. 不妨设为 $\alpha_i<\beta_i$，但与 $\beta\leq_{lex}\alpha$ 相矛盾. 现证传递性，假设 $\alpha<_{lex}\beta$，$\beta<_{lex}\gamma$(只须考虑严格不等关系情形)，这样就有 $\alpha_1=\beta_1$，…，$\alpha_{i-1}=\beta_{i-1}$ 且 $\alpha_i<\beta_i$. 设 γ_p 为满足 $\beta_p<\gamma_p$ 的第一个坐标. 若 $p<i$，则

$$\gamma_1=\beta_1=\alpha_1,\cdots,\gamma_{p-1}=\beta_{p-1}=\alpha_{p-1},\alpha_p=\beta_p<\gamma_p;$$

若 $p\geqslant i$，则

561 $$\gamma_1=\beta_1=\alpha_1,\cdots,\gamma_{i-1}=\beta_{i-1}=\alpha_{i-1},\alpha_i<\beta_i=\gamma_i.$$

在任意一种情形下，$\gamma-\alpha$ 的第一个非零的坐标都是正的，也就是 $\alpha<_{lex}\gamma$.

其次，我们证明字典序是一个良序. 设 S 是N^n 的一个非空子集，定义

$$C_1=\{S\text{ 中的所有有序 }n\text{ 元组的第一个坐标}\},$$

定义 δ_1 为 C_1 中的最小的数(注意 C_1 是良序集N的一个非空子集). 定义

$$C_2=\{\text{所有有序 }n\text{ 元组}(\delta_1,\alpha_2,\cdots,\alpha_n)\in S\text{ 的第二个坐标}\}.$$

因为 $C_2\neq\varnothing$，所以它包含一个最小的数 δ_2，类似地，对所有 $i<n$，定义 C_{i+1} 为 S 中所有开始 i 个坐标是(δ_1，δ_2，…，δ_i)的有序 n 元组的所有第 $i+1$ 个坐标构成的集合，定义 δ_{i+1} 为 C_{i+1} 中的最小整数. 由构造方法知，n 元组 $\delta=(\delta_1,\delta_2,\cdots,\delta_n)$在 S 中. 进一步，若 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in S$，则

$$\alpha-\delta=(\alpha_1-\delta_1,\alpha_2-\delta_2,\cdots,\alpha_n-\delta_n)$$

的所有坐标是非负的. 因此，若 $\alpha\neq\delta$，则它的第一个非零的坐标是正的，所以 $\delta\leq_{lex}\alpha$. 因此字典序是一个良序.

假设 $\alpha\leq_{lex}\beta$，我们断言，对所有的 $\gamma\in N$

$$\alpha+\gamma\leq_{lex}\beta+\gamma.$$

若 $\alpha=\beta$，则 $\alpha+\gamma=\beta+\gamma$；若 $\alpha<_{lex}\beta$，则 $\beta-\alpha$ 的第一个非零的坐标是正的. 但

$$(\beta+\gamma)-(\alpha+\gamma)=\beta-\alpha,$$

故 $\alpha+\gamma<_{lex}\beta+\gamma$. 因此$\leq_{lex}$是一个单项式序. ■

按照字典序，$x_1>x_2>x_3>\cdots$，因为

$$(1,0,\cdots,0)\prec(0,1,0,\cdots,0)\prec(0,0,1,0,\cdots,0)\prec\cdots.$$

变量 $x_{\sigma(1)}$，…，$x_{\sigma(n)}$的任意一个置换产生N^n 上的一个不同的字典序.

注 设 X 是一个带有序$\leq$的良序的集合，则 X^n 上的字典序可定义为：$a=(a_1,\cdots,a_n)\leq_{lex}b=(b_1,\cdots,b_n)$当 $a=b$ 或它们第一个不相同的坐标是第 i 个且 $a_i<b_i$. 若用
562 X 代替N，推广命题 7.45 是一件简单的事情.

定义 设 X 是一个集且 $n\geqslant1$，我们定义 X 上长为 n 的**正字** w 为一个函数 $w:\{1,2,\cdots,n\}\to X$，记 w 为

$$w = x_1 x_2 \cdots x_n,$$

其中 $x_i = w(i)$. 当然，我们不需要单射，即可能存在重复的 x. 两个正字可以相乘：若 $w' = x_1' \cdots x_m'$，则

$$ww' = x_1 x_2 \cdots x_n x_1' \cdots x_m'.$$

我们引入**空字**，它是长为零的字，记为 1，而且对所有正字 w 有 $1w = w = w1$. 在这些定义下，由所有空字及集合 X 上的所有正字构成的集合$\mathcal{W}(X)$就是一个幺半群.

推论 7.55 设 X 是一个良序集，则按字典序(我们记为 $\leq_{\text{lex}}$)，$\mathcal{W}(X)$是良序的.

证明 我们这里只是给出字典序的详细定义，它是良序的证明留给读者. 首先，对所有 $w \in \mathcal{W}(X)$，定义 $1 \leq_{\text{lex}} w$. 其次，对给定的$\mathcal{W}(X)$中的字 $u = x_1 \cdots x_p$ 和 $v = y_1 \cdots y_q$，在短的字的末尾处添加一些 1 使得它们的长度一样，并重新命名为$\mathcal{W}(X)$中的 u'，v'. 若 $m \geq \max\{p, q\}$，则我们可视 u'，$v' \in X^m$. 我们定义 $u \leq_{\text{lex}} v$ 若在 X^m 中 $u' \leq_{\text{lex}} v'$(这是在字典中通常使用的序，在字典中，空白是在任何字母的前面：例如，muse 排在 museum 之前). ■

例 7.56 给定$\mathbb{N}^n$ 上的一个单项式序，每一个多项式 $f(X) = \sum_{\alpha} c_\alpha X^\alpha \in k[X] = k[x_1, \cdots, x_n]$都可以按照它的项的多重次数写成下降的顺序：$\alpha_1 > \alpha_2 > \cdots > \alpha_p$. 记

$$\text{multiword}(f) = \alpha_1 \cdots \alpha_p \in \mathcal{W}(\mathbb{N}^n).$$

设 $c_\beta X^\beta$ 为 $f(X)$中的一个非零的项，$g(X) \in k[X]$满足 $\text{DEG}(g) < \beta$，并记

$$f(X) = h(X) + c_\beta X^\beta + \ell(X),$$

其中 $h(X)$是 $f(X)$中多重次数$>\beta$的项的和，$\ell(X)$是 $f(X)$中多重次数$<\beta$的项的和. 我们断言，在$\mathcal{W}(X)$中，

$$\text{multiword}(f(X) - c_\beta X^\beta + g(X)) <_{\text{lex}} \text{multiword}(f).$$

$f(X) - c_\beta X^\beta + g(X)$中满足多重次数$>\beta$的项的和是 $h(X)$，而次数更低的项的和是 $\ell(X) + g(X)$. 但由习题 7.51 中 $\text{DEG}(\ell + g) < \beta$. 因此 $f(X)$和 $f(X) - c_\beta X^\beta + g(X)$的初始项是相同的，而 $f(X) - c_\beta X^\beta + g(X)$的下一项的多重次数$<\beta$，这就证明了这个论断.

若 $f(X) \to f(X) - c_\beta X^\beta + g(X)$，其中 $c_\beta X^\beta$ 是 $f(X)$的非零项且 $\text{DEG}(g) < \beta$，则 $f(X) >_{\text{lex}} f(X) - c_\beta X^\beta + g(X)$. 因为$\mathcal{W}(\mathbb{N}^n)$是良序的，由此得出，这样形式的序列一定是有限的. ◀ 563

下面是第二种通用的单项式序.

定义 $\mathbb{N}^n$ 上的**次数-字典序**定义为：$\alpha \leq_{\text{dlex}} \beta$ 若 $\alpha = \beta$ 或

$$|\alpha| = \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i = |\beta|,$$

或，若 $|\alpha| = |\beta|$，则 $\beta - \alpha$ 的第一个非零的坐标是正的.

换言之，给定 $\alpha = (\alpha_1, \cdots, \alpha_n)$和 $\beta = (\beta_1, \cdots, \beta_n)$，首先检查总次数：若 $|\alpha| < |\beta|$，则 $\alpha \leq_{\text{dlex}} \beta$；若 α，β的总次数相同，则用字典方式给它们排序. 例如$(1, 2, 3, 0) <_{\text{dlex}} (0, 2, 5, 0)$且$(1, 2, 3, 4) <_{\text{dlex}} (1, 2, 5, 2)$.

命题 7.57 次数-字典序$\leq_{\text{dlex}}$是$\mathbb{N}^n$ 上的一个单项式序.

证明 按照通常的方法就可证明$\leq_{\text{dlex}}$是$\mathbb{N}^n$ 上的一个偏序. 下面证明它是一个良序. 设 S 是$\mathbb{N}^n$ 的一个非空子集. S 中的元的总次数全体形成$\mathbb{N}$ 的一个非空子集，故存在一个最小者，

不妨设为 t. 而所有具有总次数 t 的 $\alpha\in S$ 构成的非空子集有一个最小元，因为在此子集上，次数一字典序就是字典序了. 因此按次数一字典序，S 中存在最小元.

假设 $\alpha\preceq_{\mathrm{dlex}}\beta$，$\gamma\in\mathbf{N}^n$. 由于 $|\alpha+\gamma|=|\alpha|+|\gamma|$，故由 $|\alpha|=|\beta|$ 可推出 $|\alpha+\gamma|=|\beta+\gamma|$ 且由 $|\alpha|<|\beta|$ 可推出 $|\alpha+\gamma|<|\beta+\gamma|$，在后一种情形时，命题 6.44 表明了 $\alpha+\gamma\preceq_{\mathrm{dlex}}\beta+\gamma$. ■

下一个命题表明，在单项式序下，多变量的多项式表现得同单变量的多项式一样.

命题 7.58 设 $\preceq$ 是 $\mathbf{N}^n$ 上的一个单项式序，$f(X)$，$g(X)$，$h(X)\in k[X]=k[x_1,\cdots,x_n]$.

(i) 若 $\mathrm{DEG}(f)=\mathrm{DEG}(g)$，则 $\mathrm{LT}(g)\mid\mathrm{LT}(f)$.

(ii) $\mathrm{LT}(hg)=\mathrm{LT}(h)\mathrm{LT}(g)$.

(iii) 若 $\mathrm{DEG}(f)=\mathrm{DEG}(hg)$，则 $\mathrm{LT}(g)\mid\mathrm{LT}(f)$.

证明 (i) $\mathrm{DEG}(f)=\alpha=\mathrm{DEG}(g)$，则 $\mathrm{LT}(f)=cX^\alpha$ 且 $\mathrm{LT}(g)=dX^\alpha$，因此 $\mathrm{LT}(g)\mid\mathrm{LT}(f)$ [也有 $\mathrm{LT}(f)\mid\mathrm{LT}(g)$].

(ii) 设 $h(X)=bX^\gamma+$低次项，$h(X)=cX^\beta+$低次项. 故 $\mathrm{LT}(h)=cX^\gamma$，$\mathrm{LT}(g)=bX^\beta$；显然 $cbX^{\gamma+\beta}$为 $h(X)g(X)$的一个非零的项. 下面证明它是 $h(X)g(X)$的首项. 设 $c_\mu X^\mu$ 为 $h(X)$的满
564 足$\mu\prec\gamma$ 的任意一项，$b_\nu X^\nu$ 是 $g(X)$的满足 $\nu\prec\beta$ 的一项. $\mathrm{DEG}(c_\mu X^\mu b_\nu X^\nu)=\mu+\nu$. 因为$\preceq$是一个单项式序，所以 $\mu+\nu\prec\gamma+\nu\prec\gamma+\beta$. 因此 $cbX^{\gamma+\beta}$是 $h(X)g(X)$中具有最大多重次数的首项.

(iii) 因为 $\mathrm{DEG}(f)=\mathrm{DEG}(hg)$，由 (i) 有 $\mathrm{LT}(hg)\mid\mathrm{LT}(f)$，由 (ii) 有 $\mathrm{LT}(h)\mathrm{LT}(g)=\mathrm{LT}(hg)$，因此 $\mathrm{LT}(g)\mid\mathrm{LT}(f)$. ■

习题

7.49 (i) 写出 $k[x,y]$中在字典序及次数-字典序下的开始的 10 个首一单项式.

(ii) 写出 $k[x,y,z]$中在字典序及次数-字典序下的总次数至多为 2 的所有首一单项式.

7.50 试给出一个良序集 X 的例子，使之包含一个有无限多个前序元的元素 u.

*7.51 设$\preceq$是$\mathbf{N}^n$ 上的一个单项式序，$f(X)$，$g(X)\in k[X]=k[x_1,\cdots,x_n]$是非零多项式. 试证，若 $f+g\neq 0$，则

$$\mathrm{DEG}(f+g)\preceq\max\{\mathrm{DEG}(f),\mathrm{DEG}(g)\},$$

且只有当 $\mathrm{DEG}(f)=\mathrm{DEG}(g)$时，严格不等式才可能出现.

7.5.2 除法算式

我们现在来用单项式序给出多个变量的多项式的除法算式.

定义 设$\preceq$为$\mathbf{N}^n$ 上的一个单项式序，$f(X)$，$g(X)\in k[X]=k[x_1,\cdots,x_n]$. 若存在 $f(X)$中的一个非零项 $c_\beta X^\beta$ 使得 $\mathrm{LT}(g)\mid C_\beta X^\beta$ 且

$$h(X)=f(X)-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}g(X),$$

则简化 $f\xrightarrow{g}h$ 表示用 h 替换 f.

简化就是单变量多项式的长除法中的通常步骤. 若 $f\xrightarrow{g}h$，则我们用 g 消去 f 中的一项就产生了h. 当然，简化中的一个特殊情形是 $c_\beta X^\beta=\mathrm{LT}(f)$时.

命题 7.59 设$\preceq$为$\mathbf{N}^n$ 上的一个单项式序，$f(X)$，$g(X)\in k[X]=k[x_1,\cdots,x_n]$. 假设

$f \xrightarrow{g} h$，也就是，存在 $f(X)$ 的一个非零项 $c_\beta X^\beta$ 使得 $\mathrm{LT}(g) \mid c_\beta X^\beta$，且 $h(X)=f(X)-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}$
$g(X)$. 565

若 $\beta=\mathrm{DEG}(f)$，则

$$h(X)=0 \text{ 或 } \mathrm{DEG}(h) \prec \mathrm{DEG}(f);$$

若 $\beta \prec \mathrm{DEG}(f)$，则 $\mathrm{DEG}(h)=\mathrm{DEG}(f)$. 在任意一种情形下，均有

$$\mathrm{DEG}\left(\frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X)\right) \preceq \mathrm{DEG}(f).$$

证明 记

$$f(X)=\mathrm{LT}(f)+c_\kappa X^\kappa+\text{低次项}.$$

因为 $c_\beta X^\beta$ 为 $f(X)$ 的一项，故有 $\beta \preceq \mathrm{DEG}(f)$. 若 $\mathrm{LT}(g)=a_\gamma X^\gamma$，故 $\mathrm{DEG}(g)=\gamma$. 记

$$g(X)=a_\gamma X^\gamma+a_\lambda X^\lambda+\text{低次项}.$$

因此

$$\begin{aligned} h(X) &= f(X)-\frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X) \\ &= f(X)-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[\mathrm{LT}(g)+a_\lambda X^\lambda+\cdots\right] \\ &= \left[f(X)-c_\beta X^\beta\right]-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[a_\lambda X^\lambda+\cdots\right]. \end{aligned}$$

由 $\mathrm{LT}(g) \mid c_\beta X^\beta$ 可知 $\beta-\gamma \in \mathbb{N}^n$. 我们断言

$$\mathrm{DEG}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[a_\lambda X^\lambda+\cdots\right]\right)=\lambda+\beta-\gamma \prec \beta.$$

上面不等式成立，因为由 $\lambda \prec \gamma$ 可推出 $\lambda+(\beta-\gamma) \prec \gamma+(\beta-\gamma)=\beta$. 下面证明 $\lambda+\beta-\gamma$ 为次数，只须证明 $\lambda+\beta-\gamma=\mathrm{DEG}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)} a_\lambda X^\lambda\right)$ 为出现在 $-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[a_\lambda X^\lambda+\cdots\right]$ 中的最大的多重次数. 但若 $a_\eta X^\eta$ 为 $g(X)$ 中的次数更低的项，即 $\eta \prec \lambda$，那么由 $\preceq$ 是一个单项式序可得 $\eta+(\beta-\gamma) \prec \lambda+(\beta-\gamma)$，得证.

若 $h(X) \neq 0$，那么由下习题 7.51 可得出

$$\mathrm{DEG}(h) \preceq \max\left\{\mathrm{DEG}\left(f(X)-c_\beta X^\beta\right), \mathrm{DEG}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[a_\lambda X^\lambda+\cdots\right]\right)\right\}.$$ 566

若 $\beta=\mathrm{DEG}(f)$，则 $c_\beta X^\beta=\mathrm{LT}(f)$，

$$f(X)-c_\beta X^\beta=f(X)-\mathrm{LT}(f)=c_\kappa X^\kappa+\text{次数更低项}.$$

因此 $\mathrm{DEG}(f(X)-c_\beta X^\beta)=\kappa \prec \mathrm{DEG}(f)$. 从而此时有 $\mathrm{DEG}(h) \prec \mathrm{DEG}(f)$. 若 $\beta \prec \mathrm{DEG}(f)$，则 $\mathrm{DEG}(f(X)-c_\beta X^\beta)=\mathrm{DEG}(f)$，而 $\mathrm{DEG}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[a_\lambda X^\lambda+\cdots\right]\right) \prec \beta \prec \mathrm{DEG}(f)$，故此时有 $\mathrm{DEG}(h)=\mathrm{DEG}(f)$.

最后的不等式是很清楚的，因为

$$\frac{c_\beta X^\beta}{\mathrm{LT}(g)} g(X)=c_\beta X^\beta+\frac{c_\beta X^\beta}{\mathrm{LT}(g)}\left[a_\lambda X^\lambda+\cdots\right].$$

因为 $\mathrm{DEG}\left(-\frac{c_\beta X^\beta}{\mathrm{LT}(g)}[a_\lambda X^\lambda+\cdots]\right)<\beta$，我们看到

$$\mathrm{DEG}\left(\frac{c_\beta X^\beta}{\mathrm{LT}(g)}g(X)\right)=\beta\leq\mathrm{DEG}(f).$$ ■

定义 设 $\{g_1,\cdots,g_m\}$，其中 $g_i=g_i(X)\in k[X]$，多项式 $r(X)$ 称为 $\bmod\{g_1,\cdots,g_m\}$**既约的**若 $r(X)=0$ 或没有 $\mathrm{LT}(g_i)$ 能整除 $r(X)$ 的任意非零项.

下面给出多变量多项式的除法算式. 因为这个算律要求"因式多项式"$\{g_1,\cdots,g_m\}$按一定的顺序使用(总之，一个算律必须给出明确的指示). 我们将用多项式的 m 元有序组这个概念而不是多项式的一个子集. 我们用记号 $[g_1,\cdots,g_m]$ 表示第 i 个分量为 g_i 的 m 元有序组，因为通常的记号 $(g_1,\cdots,g_m)$ 将会与由所有 g_i 生成的理想 $(g_1,\cdots,g_m)$ 相混淆.

定理 7.60($k[x_1,\cdots,x_n]$ 中的除法算式) 设 $\preceq$ 为 $\mathbb{N}^n$ 上的一个单项式序，$k[X]=k[x_1,\cdots,x_n]$. 若 $f(X)\in k[X]$ 且 $G=[g_1(X),\cdots,g_m(X)]$ 是 $k[X]$ 上的一个多项式的 m 元有序组，则存在一个算律，它能给出多项式 $r(X),a_1(X),\cdots,a_m(X)\in k[X]$ 使得

$$f=a_1g_1+\cdots+a_mg_m+r,$$

其中 r 是 $\bmod\{g_1,\cdots,g_m\}$ 既约的，且对所有 i 有 $\mathrm{DEG}(a_ig_i)\preceq\mathrm{DEG}(f)$.

证明 一个单项式序选定后，多项式的首项就确定了，此算律是单变量的多项式的除法算式的直接推广. 首先尽可能多地 mod g_1 约化，再 mod g_2 约化，再 mod g_3 约化，等等. 下面

567 有一个更准确描述这个算律的编码：

```
Input: f(X) = Σ_β c_β X^β, [g_1, …, g_m]
Output: r, a_1, …, a_m
r := f; a_i := 0
WHILE f is not reduced mod {g_1, …, g_m} DO
  select smallest i with LT(g_i) | c_β X^β for some β
  f − [c_β X^β / LT(g_i)] g_i := f
  a_i + [c_β X^β / LT(g_i)] := a_i
END WHILE
```

在此算律的每一步骤 $h_j\xrightarrow{g_i}h_{j+1}$ 中，由例 7.56，在 $\mathcal{W}(\mathbb{N}^n)$ 中，我们有 $\mathrm{multiword}(h_j)\succ_{\mathrm{lex}}\mathrm{miltiword}(h_{j+1})$. 故算律会停止因为 $\prec_{\mathrm{lex}}$ 是 $\mathcal{W}(\mathbb{N}^n)$ 上的一个良序. 显然，输出项 $r(X)$ 是 $\bmod\{g_1,\cdots,g_m\}$ 既约的，因为若它有一项被某 $\mathrm{LT}(g_i)$ 整除，则就有更进一步的约化.

最后，对某中间输出项 $h(X)$，$a_i(X)$ 的每一项都具有形式 $c_\beta X^\beta/\mathrm{LT}(g_i)$(像人们在编码中看到的). 由命题 7.59 知，或者 $a_ig_i=0$ 或者 $\mathrm{DEG}(a_ig_i)\prec\mathrm{DEG}(f)$. ■

定义 给定 $\mathbb{N}^n$ 的一个单项式序，一个多项式 $f(X)\in k[X]$，及一个 m 元有序组 $G=[g_1,\cdots,g_m]$，我们称除法算式的输出项 $r(X)$ 为 ***f* mod G 的余式**.

注意 f mod G 的余式 r 是 $\bmod\{g_1,\cdots,g_m\}$ 既约的，且 $f-r\in I=(g_1,\cdots,g_m)$. 算律要求 G 为一个 m 元有序组，这是因为命令

select smallest i with $\mathrm{LT}(g_i)\mid c_\beta X^\beta$ for some β

就指明了约化的序. 下一个例子表明，余式不仅依靠多项式集$\{g_1, \cdots, g_m\}$，而且依靠 m 元有序组$G=[g_1, \cdots, g_m]$中分量的排序，也就是说，若$\sigma \in S_m$是一个置换且$G_\sigma=[g_{\sigma(1)}, \cdots, g_{\sigma(m)}]$，则 f mod G_σ 的余式 r_σ 可能与 f mod G 的余式 r 不相等，甚至更糟的是，有可能$r \neq 0$ 而$r_\sigma=0$，因此 mod G 的余式不是 f 在理想$(g_1, \cdots, g_m)$中的阻碍.

例 7.61 设 $f(x, y, z)=x^2y^2+xy$，设 $G=[g_1, g_2, g_3]$，其中

$$g_1 = y^2+z^2$$
$$g_2 = x^2y+yz$$
$$g_3 = z^3+xy$$

我们使用$\mathbb{N}^3$ 上的次数一字典序. 由于 $y^2=\mathrm{LT}(g_1) \mid \mathrm{LT}(f)=x^2y^2$，故 $f \xrightarrow{g_1} h$，其中 $h=f-\frac{x^2y^2}{y^2}(y^2+z^2)=-x^2z^2+xy$. 多项式$-x^2z^2+xy$ 是 mod G 既约的，因为$-x^2z^2$，xy 不被首项 568
$\mathrm{LT}(g_1)=y^2$，$\mathrm{LT}(g_2)=x^2y$ 及 $\mathrm{LT}(g_3)=z^3$ 中的任一个整除.

另一方面，让我们以 3 元有序组 $G'=[g_2, g_1, g_3]$来应用一下面的除法算式. 则第一个约化给出 $f \xrightarrow{g_2} h'$，其中

$$h' = f-\frac{x^2y^2}{x^2y}(x^2y+yz) = -y^2z+xy.$$

注意 h'不是既约的，mod g_1 约化之，给出

$$h'-\frac{-y^2z}{y^2}(y^2+z^2) = z^3+xy.$$

但 $z^3+xy=g_3$，故 $z^3+xy \xrightarrow{g_3} 0$.

因此余式依赖于 m 元有序组中因式多项式 g_i 的排序.

对于一个更简单的有不同的余式(均不为 0)的例子，请参阅习题 7.52. ◀

余式对 m 元有序组 $G=[g_1, \cdots, g_m]$中 g_i 顺序的依赖性将在下一小节中讨论.

习题

*7.52 设 $G=[x-y, x-z]$，$G'=[x-z, x-y]$. 试证 x mod G 与 x mod G'(次数-字典序)的余式是不同的.

7.53 在此习题中用次数一字典序.

(i)求 $x^7y^2+x^3y^2-y+1$ mod $[xy^2-x, x-y^3]$的余式.

(ii)求 $x^7y^2+x^3y^2-y+1$ mod $[x-y^3, xy^2-x]$的余式.

7.54 在此习题中用次数一字典序.

(i)求 $x^2y+xy^2+y^2$ mod $[y^2-1, xy-1]$的余式.

(ii)求 $x^2y+xy^2+y^2$ mod $[xy-1, y^2-1]$的余式.

*7.55 设 $c_\alpha X^\alpha$ 是一个非零的单项式，多项式 $f(X)$，$g(X) \in k[X]$的没有一个非零项能被 $c_\alpha X^\alpha$ 整除. 试证 $f(X)-g(X)$没有一个非零项能被 $c_\alpha X^\alpha$ 整除.

*7.56 $k[X]$中的一个理想 I 是一个**单项式理想**，若它是由一些单项式生成的理想：$I=(X^{\alpha(1)}, \cdots, X^{\alpha(q)})$.

(i)试证 $f(X) \in I$ 当且仅当 $f(X)$的每一项都可被某 $X^{\alpha(i)}$ 整除.

(ii)试证若 $G=[g_1, \cdots, g_m]$且 r 是 mod G 既约的，则 r 不在单项式理想$(\mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_m))$中. 569

7.6 格罗布纳基

在此节中，涉及余式时，我们假设$\mathbb{N}^n$带有某个单项式序(读者可用次数-字典序)，故LT(f)有定义且除法算式有意义.

我们看到，由除法算式而得的 f mod $[g_1, \cdots, g_m]$的余式依赖于 g_i 的排列. 理想 $I=(g_1, \cdots, g_m)$的格罗布纳基(Gröbner basis)就是一组满足下列性质的基：对任意一个由 g_i 组成的m 元有序组G，f mod G 的余式确定了 f 是否在 I 中，这将是定义的一个推论(给出定义是为了确保格罗布纳基是集合而不是 m 元有序组).

定义 称多项式集$\{g_1, \cdots, g_m\}$是理想 $I=(g_1, \cdots, g_m)$的一个**格罗布纳**[⊖]基，若对每一个非零 $f\in I$，存在某 g_i 使得 $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$.

例 7.61 表明

$$\{y^2+z^2, x^2y+yz, z^3+xy\}$$

不是理想 $I=(y^2+z^2, x^2y+yz, z^3+xy)$的一个格罗布纳基.

命题 7.62 多项式集$\{g_1, \cdots, g_m\}$是理想 $I=(g_1, \cdots, g_m)$的一个格罗布纳基当且仅当对每一个 m 元有序组$G_\sigma=[g_{\sigma(1)}, \cdots, g_{\sigma(m)}]$(其中 $\sigma\in S_m$)，每一个 $f\in I$ 的余式是 0 mod G_σ.

证明 假设存在某置换 $\sigma\in S_m$ 及某 $f\in I$ 使得 f mod G_σ 的余式不为 0. 在所有这样的多项式中，选择 f 使之具有最小的次数. 因为$\{g_1, \cdots, g_m\}$是一个格罗布纳基，故对某 i 有 $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$. 在存在简化 $f\xrightarrow{g_{\sigma(i)}}h$ 的 $\sigma(i)$中选择最小者，注意 $h\in I$. 因为 $\mathrm{DEG}(h)\prec\mathrm{DEG}(f)$，故由命题 7.59，除法算式给出一系列简化 $h=h_0\to h_1\to h_2\to\cdots\to h_p=0$. 对 f 应用除法算式知可在此系列简化之前添加 $f\to h$，由此得出 f mod G_σ 的余式是 0，矛盾！

反之，设$\{g_1, \cdots, g_m\}$是 $I=(g_1, \cdots, g_m)$的一个格罗布纳基. 若对每一个 i 存在一个非零 $f\in I$ 使得 $\mathrm{LT}(g_i)\nmid\mathrm{LT}(f)$，则在任意一个简化 $f\xrightarrow{g_i}h$ 中，我们有 $\mathrm{LT}(h)=\mathrm{LT}(f)$. 因此，若$G=[g_1, \cdots, g_m]$，则在 mod G 下应用除法算式就给出简化 $f\to h_1\to h_2\to\cdots\to h_p=r$ 且
570 $\mathrm{LT}(r)=\mathrm{LT}(f)$. 因此，$r\neq 0$，也就是说 f mod G 的余式不是 0，矛盾. ■

推论 7.63 设 $I=(g_1, \cdots, g_m)$为一个理想，设$\{g_1, \cdots, g_m\}$为 I 的一个格罗布纳基，且设 $G=[g_1, \cdots, g_m]$为由 g_i 构成的任意一个 m 元有序组. 若 $f(X)\in k[X]$，则存在唯一的 $r(X)\in k[X]$使得 $f-r\in I$，其中 $r(X)$是 mod$\{g_1, \cdots, g_m\}$既约的. 事实上，$r(X)$是 f mod G 的余式.

证明 除法算式给出了一个 mod$\{g_1, \cdots, g_m\}$既约的多项式 r 及满足 $f=a_1g_1+\cdots+a_mg_m+r$ 的多项式 $a_1, \cdots, a_m$. 显然，$f-r=a_1g_1+\cdots+a_mg_m\in I$.

下面证明唯一性. 假设 r 和 r'是 mod$\{g_1, \cdots, g_m\}$既约的且 $f-r$ 和 $f-r'$均在 I 中，故$(f-r')-(f-r)=r-r'\in I$. 因为 r 和 r'都是 mod$\{g_1, \cdots, g_m\}$既约的，它们中没有一项能被任何 $\mathrm{LT}(g_i)$整除. 若 $r-r'\neq 0$，那么由习题 7.55 知，$r-r'$中没有一项能被任何 $\mathrm{LT}(g_i)$整除.

⊖ 是布切贝哥(B. Buchberger)在他的学位论文中证明了格罗布纳基的主要性质，他这样命名是为了表示对他的导师格罗布纳的尊重.

特别地，$\mathrm{LT}(r-r')$不被任何$\mathrm{LT}(g_i)$整除，这与命题7.62矛盾！因此$r=r'$. ■

下面的推论表明，格罗布纳基解决了在除法算式中用不同的m元有序组得到不同余式的问题.

推论 7.64 设$I=(g_1, \cdots, g_m)$为一个理想，$\{g_1, \cdots, g_m\}$为I的一个格罗布纳基，G为m元有序组$G=[g_1, \cdots, g_m]$.

(i)若$f(X)\in k[X]$，$G_\sigma=[g_{\sigma(1)}, \cdots, g_{\sigma(m)}]$，其中$\sigma\in S_m$是一个置换，则$f \bmod G$的余式等于$f \bmod G_\sigma$的余式.

(ii)多项式$f\in I$当且仅当$f \bmod G$的余式为0.

证明 (i)若r是$f \bmod G$的余式，那么由推论7.63知r是满足$f-r\in I$和$\bmod\{g_1, \cdots, g_m\}$既约的唯一多项式. 类似地，$f \bmod G_\sigma$的余式$r_\sigma$是满足$f-r_\sigma\in I$和$\bmod G_\sigma$既约的唯一多项式，由推论7.63的唯一性知$r=r_\sigma$.

(ii)命题7.62表明，若$f\in I$，则它的余式是0. 反之，若r是$f \bmod G$的余式，则$f=q+r$，其中$q\in I$. 因此，若$r=0$，则$f\in I$. ■

许多明显的问题出现了. 格罗布纳基存在吗？若存在，唯一吗？给定$k[X]$中的一个理想I，存在会使我们认识求I的格罗布纳基的算式吗？

术语S-多项式会使我们认识格罗布纳基，但我们首先引入一些记号.

定义 设$\alpha=(\alpha_1, \cdots, \alpha_n)$和$\beta=(\beta_1, \cdots, \beta_n)$都在$\mathbb{N}^n$中，定义

$$\alpha \vee \beta = \mu,$$

其中$\mu=(\mu_1, \cdots, \mu_n)$由$\mu_i=\max\{\alpha_i, \beta_i\}$给出. 571

易见$X^{\alpha\vee\beta}$是单项式X^α和X^β的最小公倍式.

定义 设$f(X)$，$g(X)\in k[X]$，其中$\mathrm{LT}(f)=a_\alpha X^\alpha$，$\mathrm{LT}(g)=b_\beta X^\beta$，定义

$$L(f,g) = X^{\alpha\vee\beta}.$$

S-多项式$S(f, g)$定义如下：

$$S(f,g) = \frac{L(f,g)}{\mathrm{LT}(f)}f - \frac{L(f,g)}{\mathrm{LT}(g)}g$$
$$= a_\alpha^{-1}X^{(\alpha\vee\beta)-\alpha}f(X) - b_\beta^{-1}X^{(\alpha\vee\beta)-\beta}g(X).$$

注意$S(f, g)=-S(g, f)$.

例 7.65 我们来证明，若$f=X^\alpha$和$g=X^\beta$是单项式，则$S(f, g)=0$. 因为f和g是单项式，所以我们有$\mathrm{LT}(f)=f$和$\mathrm{LT}(g)=g$. 因此

$$S(f,g) = \frac{L(f,g)}{\mathrm{LT}(f)}f - \frac{L(f,g)}{\mathrm{LT}(g)}g = \frac{X^{\alpha\vee\beta}}{f}f - \frac{X^{\alpha\vee\beta}}{g}g = 0.$$ ◀

下面这个技术的引理指出了为什么S-多项式与我们的讨论是相关的.

引理 7.66 给定$g_1(X), \cdots, g_\ell(X)\in k[X]$和单项式$c_jX^{\alpha(j)}$. 设$h(X)=\sum_{j=1}^{\ell} c_jX^{\alpha(j)}g_j(X)$.

设δ是一个多重次数. 若$\mathrm{DEG}(h)<\delta$且对所有的$j<\ell$，$\mathrm{DEG}(c_jX^{\alpha(j)}g_j(X))=\delta$，则存在$d_j\in k$使得

$$h(X) = \sum_j d_jX^{\delta-\mu(j)}S(g_j, g_{j+1}),$$

其中 $\mu(j)=\mathrm{DEG}(g_j)\vee\mathrm{DEG}(g_{j+1})$，且对所有 $j<\ell$，

$$\mathrm{DEG}(X^{\delta-\mu(j)}S(g_j,g_{j+1}))<\delta.$$

注 此引理说，若 $\mathrm{DEG}\left(\sum_j a_jg_j\right)<\delta$，其中 a_j 是单项式，而对所有 j，$\mathrm{DEG}(a_jg_j)=\delta$，则 h 可写成 S-多项式的一个线性组合，此线性组合以单项式作为系数且每一项的

572 多重次数严格小于 δ.

证明 设 $\mathrm{LT}(g_j)=b_jX^{\beta(j)}$，故 $\mathrm{LT}(c_jX^{\alpha(j)}g_j(X))=c_jb_jX^{\delta}$. 因此 $h(X)$ 中 X^{δ} 的系数是 $\sum_j c_jb_j$. 因为 $\mathrm{DEG}(h)<\delta$，我们必须有 $\sum_j c_jb_j=0$. 定义首一多项式

$$u_j(X)=b_j^{-1}X^{\alpha(j)}g_j(X).$$

存在和

$$\begin{aligned}h(X)&=\sum_{j=1}^{\ell}c_jX^{\alpha(j)}g_j(X)\\&=\sum_{j=1}^{\ell}c_jb_ju_j\\&=c_1b_1(u_1-u_2)+(c_1b_1+c_2b_2)(u_2-u_3)+\cdots\\&\quad+(c_1b_1+\cdots+c_{\ell-1}b_{\ell-1})(u_{\ell-1}-u_\ell)\\&\quad+(c_1b_1+\cdots+c_\ell b_\ell)u_\ell.\end{aligned}$$

因为 $\sum_j c_jb_j=0$，所以最后一项 $(c_1b_1+\cdots+c_\ell b_\ell)u_\ell=0$. 因为 $\mathrm{DEG}(c_jX^{\alpha(j)}g_j(X))=\delta$，所以我们有 $\alpha(j)+\beta(j)=\delta$，因此对所有 j 有 $X^{\beta(j)}\mid X^{\delta}$. 因此，对所有 $j<\ell$，我们有 $\mathrm{lcm}\{X^{\beta(j)},X^{\beta(j+1)}\}=X^{\beta(j)\vee\beta(j+1)}\mid X^{\delta}$. 也就是说，若我们记 $\mu(j)=\beta(j)\vee\beta(j+1)$，则 $\delta-\mu(j)\in\mathbb{N}^n$. 但

$$\begin{aligned}X^{\delta-\mu(j)}S(g_j,g_{j+1})&=X^{\delta-\mu(j)}\left(\frac{X^{\mu(j)}}{\mathrm{LT}(g_j)}g_j(X)-\frac{X^{\mu(j)}}{\mathrm{LT}(g_{j+1})}g_{j+1}(X)\right)\\&=\frac{X^{\delta}}{\mathrm{LT}(g_j)}g_j(X)-\frac{X^{\delta}}{\mathrm{LT}(g_{j+1})}g_{j+1}(X)\\&=b_j^{-1}X^{\alpha(j)}g_j-b_{j+1}^{-1}X^{\alpha(j+1)}g_{j+1}\\&=u_j-u_{j+1}.\end{aligned}$$

在和式中代入此等式，即得出我们所希望的形式：

$$\begin{aligned}h(X)&=c_1b_1X^{\delta-\mu(1)}S(g_1,g_2)+(c_1b_1+c_2b_2)X^{\delta-\mu(2)}S(g_2,g_3)+\cdots\\&\quad+(c_1b_1+\cdots+c_{\ell-1}b_{\ell-1})X^{\delta-\mu(\ell-1)}S(g_{\ell-1},g_\ell).\end{aligned}$$

其中 $d_j=c_1b_1+\cdots+c_jb_j$.

最后，因为 u_j 和 u_{j+1} 都是首项的多重次数均为 δ 的首一多项式，所以我们有 $\mathrm{DEG}(u_j-u_{j+1})<\delta$. 但我们已经证明了 $u_j-u_{j+1}=X^{\delta-\mu(j)}S(g_j,g_{j+1})$，故 $\mathrm{DEG}(X^{\delta-\mu(j)}S(g_j,g_{j+1}))<\delta$，得证. ∎

由命题 7.62，$\{g_1,\cdots,g_m\}$ 是理想 $I=(g_1,\cdots,g_m)$ 的一个格罗布纳基，若每一个 $f\in$

573 $I \bmod G$ 的余式为 0（其中 G 是任意排列 g_j 而得的任一个 m 元有序组）. 下面定理的重要性在于，它证明了只要计算有限多个多项式，即 S-多项式，的余式，就可以确定 $\{g_1,\cdots,g_m\}$ 是

否为一个格罗布纳基.

定理 7.67(布切贝哥) 集$\{g_1, \cdots, g_m\}$是理想$I=(g_1, \cdots, g_m)$的一个格罗布纳基当且仅当对所有p, q, $S(g_p, g_q)\bmod G$的余式为 0, 其中$G=[g_1, \cdots, g_m]$.

证明 显然, 作为g_p和g_q的一个线性组合, $S(g_p, g_q)$在I中. 因此, 若$G=\{g_1, \cdots, g_m\}$是一个格罗布纳基, 那么由命题 7.62 可知$S(g_p, g_q)\bmod G$的余式是 0.

反之, 假设对所有p, q, $S(g_p, g_q)\bmod G$的余式为 0, 我们来证明每一个$f\in I \bmod G$的余式是 0. 由命题 7.62, 只需证明若$f\in I$, 则对某i, $\mathrm{LT}(g_i)\mid \mathrm{LT}(f)$. 因为$f\in I=(g_1, \cdots, g_m)$, 我们可记$f=\sum_i h_i g_i$, 故

$$\mathrm{DEG}(f)\preceq \max_i\{\mathrm{DEG}(h_i g_i)\}.$$

若对某个i有$\mathrm{DEG}(f)=\mathrm{DEG}(h_i g_i)$, 则由命题 7.58 可得$\mathrm{LT}(g_i)\mid \mathrm{LT}(f)$, 矛盾. 因此, 假设有严格不等式: $\mathrm{DEG}(f)\prec\max_i\{\mathrm{DEG}(h_i g_i)\}$.

多项式f可以用多种方式写成g_i的线性组合, 在所有形如$f=\sum_i h_i g_i$的表示中, 选择一个使得$\delta=\max_i\{\mathrm{DEG}(h_i g_i)\}$是最小者(因为$\preceq$是一个良序, 所以这是可实现的). 若$\mathrm{DEG}(f)=\delta$, 则像上面一样我们的证明完成了. 因此假设有严格不等式: $\mathrm{DEG}(f)\prec\delta$. 记

$$f=\sum_{j,\mathrm{DEG}(h_j g_j)=\delta} h_j g_j+\sum_{\ell,\mathrm{DEG}(h_\ell g_\ell)\prec\delta} h_\ell g_\ell. \tag{1}$$

若$\mathrm{DEG}\left(\sum_j h_j g_j\right)=\delta$, 则$\mathrm{DEG}(f)=\delta$, 矛盾. 因此$\mathrm{DEG}\left(\sum_j h_j g_j\right)\prec\delta$. 但这个和式中$X^\delta$的系数是从它的首项中而得的, 故

$$\mathrm{DEG}\left(\sum_j \mathrm{LT}(h_j)g_j\right)\prec\delta.$$

注意$\sum_j \mathrm{LT}(h_j)g_j$是一个满足引理 7.66 的多项式, 故存在常量$d_j$及多重次数$\mu(j)$使得

$$\sum_j \mathrm{LT}(h_j)g_j=\sum_j d_j X^{\delta-\mu(j)}S(g_j,g_{j+1}), \tag{2}$$

其中$\mathrm{DEG}(X^{\delta-\mu(j)}S(g_j, g_{j+1}))\prec\delta$⊖. 574

因为每一个$S(g_j, g_{j+1})\bmod G$的余式为 0, 由除法算式, 有$a_{ji}(X)\in k[X]$使得

$$S(g_j,g_{j+1})=\sum_i a_{ji}g_i,$$

其中对所有的j, i $\mathrm{DEG}(a_{ji}g_i)\preceq\mathrm{DEG}(S(g_j, g_{j+1}))$. 由此得出

$$X^{\delta-\mu(j)}S(g_j,g_{j+1})=\sum_i X^{\delta-\mu(j)}a_{ji}g_i.$$

因此, 由引理 7.66, 即有

$$\mathrm{DEG}(X^{\delta-\mu(j)}a_{ji})\preceq\mathrm{DEG}(X^{\delta-\mu(j)}S(g_j,g_{j+1}))\prec\delta. \tag{3}$$

⊖ 读者也许会问, 为什么我们考虑所有的S-多项式$S(g_p, g_q)$而不仅是形如$S(g_i, g_{i+1})$的那部分. 回答是, 余式条件仅应用于满足$\mathrm{DEG}(h_j g_j)=\delta$的那些$h_j g_j$, 若将指标看成$i$, 则指标不一定是连续的.

将其代入(2)，我们有

$$\begin{aligned}\sum_j \mathrm{LT}(h_j)g_j &= \sum_j d_j X^{\delta-\mu(j)} S(g_j, g_{j+1}) \\ &= \sum_j d_j \Big(\sum_i X^{\delta-\mu(j)} a_{ji} g_i\Big) \\ &= \sum_i \Big(\sum_j d_j X^{\delta-\mu(j)} a_{ji}\Big) g_i.\end{aligned}$$

若我们记 $\sum_j d_j X^{\delta-\mu(j)} a_{ji}$ 为 h_i'，则

$$\sum_j \mathrm{LT}(h_j)g_j = \sum_i h'_i g_i, \tag{4}$$

其中，由(3)有对所有的 i，$\mathrm{DEG}(h_i'g_i) < \delta$.

最后，我们将(4)中的表达式代入(1)：

$$\begin{aligned} f &= \sum_{\substack{j \\ \mathrm{DEG}(h_j g_j)=\delta}} h_j g_j + \sum_{\substack{\ell \\ \mathrm{DEG}(h_\ell g_\ell)<\delta}} h_\ell g_\ell \\ &= \sum_{\substack{j \\ \mathrm{DEG}(h_j g_j)=\delta}} \mathrm{LT}(h_j) g_j + \sum_{\substack{j \\ \mathrm{DEG}(h_j g_j)=\delta}} [h_j - \mathrm{LT}(h_j)] g_j + \sum_{\substack{\ell \\ \mathrm{DEG}(h_\ell g_\ell)<\delta}} h_\ell g_\ell \\ &= \sum_i h_i' g_i + \sum_{\substack{j \\ \mathrm{DEG}(h_j g_j)=\delta}} [h_j - \mathrm{LT}(h_j)] g_j + \sum_{\substack{\ell \\ \mathrm{DEG}(h_\ell g_\ell)<\delta}} h_\ell g_\ell. \end{aligned}$$

我们将 f 重写成 g_i 的一个线性组合，且其中每一项的多重次数严格小于 δ，这与 δ 的最小性矛
575 盾，从而完成此证明. ■

推论 7.68 若 $I=(f_1, \cdots, f_s)$ 是 $k[X]$ 中的一个单项式理想，即每一个 f_i 是一个单项式，则 $\{f_1, \cdots, f_s\}$ 是 I 的一个格罗布纳基.

证明 由例 7.65，任意一对单项式的 S-多项式都是 0. ■

下面是主要结论.

定理 7.69(布切贝哥算法) $k[X]$ 中每一个理想 $I=(f_1, \cdots, f_s)$ 都有格罗布纳基[⊖]，且可由一个算法而得.

证明 下面是一个算法的伪码.

```
Input: B={f_1, …, f_s}   G=[f_1, …, f_s]
Output: a Gröbner basis B={g_1, …, g_m}
containing{f_1, …, f_s}
B := {f_1, …, f_s};    G := [f_1, …, f_s]
REPEAT
  B' := B;    G' := G
  FOR each pair g, g' with g≠g'∈B' DO
    r := remainder of S(g, g') mod G'
```

⊖ 格罗布纳基的存在性的非构造的证明可用希尔伯特基定理的证明给出，见科克斯(Cox)、黎特(Little)及奥厦(O'Shea)的书中第 2.5 节(他们在 2.7 节中给出了一个构造性的证明).

```
IF r≠0 THEN
  B := B∪{r};    G' := [g_1, …, g_m, r]
END IF
END FOR
UNTIL B = B'
```

此算法的每一循环都将一个子集 $B\subseteq I=(g_1, \cdots, g_m)$ 增大，添加它的 S-多项式 $S(g, g')$ 中的一个的 mod G 余式至其中，因为 $g, g'\in I$，所以 $S(g, g')$ 的余式 r 在 I 中，故更大的集 $B\cup\{r\}$ 也包含于 I 中.

此算法在某 B' 处停止的唯一的阻碍是某 $S(g, g')\bmod G'$ 的余式不为 0. 因此，算法停止，则定理 7.67 表明 B' 是一个格罗布纳基.

下面证明算法的确会停止. 假设一个循环自 B' 处开始，至 B 处结束. 因为 $B'\subseteq B$，我们就有一个单项式理想的包含关系

$$(\mathrm{LT}(g') : g' \in B') \subseteq (\mathrm{LT}(g) : g \in B).$$

我们断言，若 $B'\subsetneq B$，则存在一个严格的理想间的包含关系. 假设 r 是某 S-多项式 mod B' 的一个(非零的)余式，且 $B=B'\cup\{r\}$. 由定义，余式 r 是 mod G 既约的. 故对任意 $g'\in B'$，r 的任一项都不被 $\mathrm{LT}(g')$ 整除. 因此由习题 7.56，$\mathrm{LT}(r)\notin(\mathrm{LT}(g') : g'\in B')$. 另一方面，我 576
们有 $\mathrm{LT}(r)\in(\mathrm{LT}(g) : g\in B)$. 因此，若此算法不停止，则存在一个无限的严格上升的理想链，这与希尔伯特基定理矛盾，因为 $k[X]$ 满足 ACC. ■

例 7.70 读者可证明 $B'=\{y^2+z^2, x^2y+yz, z^3+xy\}$ 不是一个格罗布纳基，因为 $S(y^2+z^2, x^2y+yz)=x^2z^2-y^2z$ mod G 的余式不为 0. 然而，添加 $x^2z^2-y^2z$ 就得出了一个格罗布纳基 B. 因为 B 中所有的 S-多项式 mod B 的余式都是 0. ◀

理论上讲，布切贝哥算法可计算出一个格罗布纳基，但如何实现它是一个问题. 在许多情形下，此算法的计算要用相当大的时间，另一方面，存在的例子表明，此算法要花费很长的时间才能得到它们输出项. 科克斯，黎特及奥厦的书第 2.9 节中讨论了布切贝哥算法的有效性.

推论 7.71 *(i)若 $I=(f_1, \cdots, f_t)$ 是 $k[X]$ 中一个理想，则存在一个决定一个多项式 $h(X)\in k[X]$ 是否在 I 中的一个算法.*

(ii)若 $I=(f_1, \cdots, f_t)$，$I'=(f_1', \cdots, f_S')$ 是 $k[X]$ 中的理想，则存在一个判断 $I=I'$ 是否成立的一个算法.

证明 (i)用布切贝哥算法求出 I 的一个格罗布纳基，再用除法算式计算 h mod G 的余式(其中 G 是由 B 中多项式排序而得的任一个 m 元有序组). 由推论 7.64(ii)知，$h\in I$ 当且仅当 $r=0$.

(ii)用布切贝哥算法分别求出 I 和 I' 的格罗布纳基 $\{g_1, \cdots, g_m\}$，$\{g_1', \cdots, g_p'\}$. 由(i)知，存在一个算法可确定是否有每一个 $g_j'\in I$ 及若每一个 $g_j'\in I$，是否有 $I'\subseteq I$. 类似地，存在一个算法可判断反包含是否成立. 故存在一个算法可确定是否有 $I=I'$ 成立. ■

这里必须注意. 推论 7.71 并不是从"若 I 是 $k[X]$ 中的一个理想"开始的，事实上，它特指一个基：$I=(f_1, \cdots, f_t)$. 当然，其原因是布切贝哥算法需要一个基作为输入项，例如，若 $J=(h_1, \cdots, h_S)$，则此算法不能用来检查是否有一个多项式 $f(X)$ 在根 $\sqrt{J}$ 中，因为人们不能

求出$\sqrt{J}$的一个基（存在算法可给出$\sqrt{(f_1, \cdots, f_t)}$的基，见贝克（Becker）和威朴分尼（Weispfenning)的书.）

一个格罗布纳基$B=\{g_1, \cdots, g_m\}$可以很大. 例如，由命题7.62知，若$f\in I$，则$B\cup$
577 $\{f\}$也是I的一个格罗布纳基. 因此，人们一般求在某种意义下最小的格罗布纳基.

定义 理想I的一个基$\{g_1, \cdots, g_m\}$是**既约的**，若

(i)每一个g_i是首一的.

(ii)每一个g_i是$\mathrm{mod}\{g_1, \cdots, \hat{g}_i, \cdots, g_m\}$既约的.

对于每一个理想$(f_1, \cdots, f_t)$，习题7.63给出了一个计算一个既约基的算法. 结合习题7.65中的算法，我们可以将一个格罗布纳基收缩为一个既约的格罗布纳基. 可以证明，一个理想的既约的格罗布纳基是唯一的.

在特殊情形下，每一个$f_i(X)$都是线性的，即

$$f_i(X) = a_{i1}x_1 + \cdots + a_{in}x_n,$$

在这个特殊情形下，公共零点$\mathrm{Var}(f_1, \cdots, f_t)$是一个$n$个未知量的$t$个方程的齐次方程组的解. 若$A=[a_{ij}]$是系数的$t\times n$矩阵，则可以证明，既约的格罗布纳基对应于矩阵$A$的既约的阶梯形式(参见贝克和威朴分尼的书中的第10.5节).

另一个特殊情形是$f_1, \cdots, f_t$是一个变量的多项式的情形. 由$\{f_1, \cdots, f_t\}$而得的既约的格罗布纳基可证明就是它们的gcd. 因此欧氏算法就被推广到了多个变量的多项式中.

最后我们来证明如何求理想的交的一个基以结束本章. 给定一个多元多项式方程组，求解的一个方法是消元(参见范德瓦尔登(van der Waerden)所著的《近世代数Ⅱ》(Modern Algebra)中的第Ⅺ章). 给定一个理想$I\subseteq k[X]$，我们导出一个关于部分未定元的理想，它实质上是带一个低维平面的$\mathrm{Var}(I)$的交.

定义 设k是一个域，设$I\subseteq k[X, Y]$为一个理想，其中$k[X, Y]$是关于不相交的变量集$X\cup Y$的多项式环. **消去理想**是

$$I_X = I \cap k[X].$$

例如，若$I=(x^2, xy)$，则格罗布纳基是$\{x^2, xy\}$(由推论7.68，因为它的生成元是单项式)，且$I_x=(x^2)\subseteq k[x]$，而$I_y=\{0\}$.

命题7.72 设k是一个域，$k[X]=k[x_1, \cdots, x_n]$有一个使得$x_1>x_2>\cdots>x_n$成立的单项式序(例如字典序)且对固定的$p>1$，设$Y=x_p, \cdots, x_n$. 若$I\subseteq k[X]$有一个格罗布纳基$G=\{g_1, \cdots, g_m\}$，则对于消去理想$I_Y=I\cap k[x_p, \cdots, x_n]$，$G\cap I_Y$是一个格罗布纳基.

证明 回忆到，$\{g_1, \cdots, g_m\}$是$I=(g_1, \cdots, g_m)$的一个格罗布纳基意味着对每一个非零的$f\in I$，存在g_i某使得$\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$. 设$f(x_p, \cdots, x_n)\in I_Y$为非零的. 因为$I_Y\subseteq I$，所以存在某$g_i(X)$使得$\mathrm{LT}(g_i)\mid\mathrm{LT}(f)$. 因此$\mathrm{LT}(g_i)$只涉及“后面”的变量$x_p, \cdots, x_n$. 设DEG
578 $(\mathrm{LT}(g_i))=\beta$. 若g_i有一项$C_\alpha X^\alpha$涉及“前面”的变量x_i，$i<P$，则因为$x_1>\cdots>x_p>\cdots>x_n$，故有$\alpha>\beta$. 这是一个矛盾，因为$\beta$是$g_i$的首项的次数，它应该比$g_i$的任何一项的次数都大. 从而$g_i\in k[x_p, \cdots, x_n]$. 习题7.62表明对于$I_Y=I\cap k[x_p, \cdots, x_n]$，$G\cap k[x_p, \cdots, x_n]$是一个格罗布纳基. ■

我们现在来给出理想交的格罗布纳基.

命题 7.73 设 k 是一个域，I_1，…，I_t 是 $k[X]$ 中的理想，其中 $X=x_1$，…，x_n.

(i)考虑 $n+t$ 个不定元的多项式环 $k[X, y_1, \cdots, y_t]$. 对所有的 j，若 J 是 $k[X, y_1, \cdots, y_t]$ 中由 $1-(y_1+\cdots+y_t)$ 和 y_jI_j 生成的理想，则 $\bigcap_{j=1}^{t} I_j=J_X$.

(ii)给定 I_1，…，I_t 的格罗布纳基，则可以计算出 $\bigcap_{j=1}^{t} I_j$ 的一个格罗布纳基.

证明 (i)若 $f=f(X)\in J_X=J\cap k[X]$，则 $f\in J$，所以有

$$f(X)=g(X, Y)(1-\sum y_j)+\sum_j h_j(X, y_1, \cdots, y_t)y_jq_j(X),$$

其中 g，$h_j\in k[X, Y]$且 $q_j\in I_j$. 设 $y_j=1$ 和其余 y 等于 0，则 $f=h_j(X, 0, \cdots, 1, \cdots, 0)q_j(X)$. 注意 $h_j(X, 0, \cdots, 1, \cdots, 0)\in k[X]$，所以 $f\in I_j$. 因为 j 是任意的，所以我们有$f\in\bigcap I_j$，从而 $J_X\subseteq\bigcap I_j$.

下面证明反包含. 若 $f\in\bigcap I_j$，则

$$f=f(1-\sum y_j)+\sum_j y_jf$$

表明 $f\in J_X$，得证.

(ii) 这可由部分(i)和命题 7.72 得出，若用单项式序，其中 X 中的所有变量先于 Y 的变量. ■

例 7.74 考虑理想 $I=(x)\cap(x^2, xy, y^2)\subseteq k[x, y]$，其中 k 是一个域. 尽管用手工求 I 的一个基是不困难的，我们用格罗布纳基来说明命题 7.73. 设 u 和 v 是新的变量，定义

$$J=(1-u-v, ux, vx^2, vxy, vy^2)\subseteq k[x,y,u,v].$$

第一步是求 J 的一个格罗布纳基. 我们用字典序，这样 $x\prec y\prec u\prec v$. 因为两个单项式的 S-多项式为 0，布切贝哥算法很快就给出 J 的一个格罗布纳基 G[⊖]： 579

$$G=\{v+u-1, x^2, yx, ux, uy^2-y^2\}.$$

由命题 7.72，I 的一个格罗布纳基是$G\cap k[x, y]$：G 中的所有不涉及 u 和 v 元素. 因此

$$I=(x)\cap(x^2,xy,y^2)=(x^2,xy).$$ ◀

习题

在下列练习中使用次数-字典单项式序.

7.57 设 $I=(y-x^2, z-x^3)$.

(i)规定序关系 $x\prec y\prec z$. 设$\preceq_{\text{lex}}$为$\mathbb{N}^3$ 上的相应的单项式序. 试证$[y-x^2, z-x^3]$不是 I 的一个格罗布纳基.

(ii)规定序关系 $y\prec z\prec x$. 设$\preceq_{\text{lex}}$为$\mathbb{N}^3$ 上的相应的单项式序. 试证$[y-x^2, z-x^3]$是 I 的一个格罗布纳基.

7.58 求 $I=(x^2-1, xy^2-x)$的一个格罗布纳基.

7.59 求 $I=(x^2+y, x^4+2x^2y+y^2+3)$的一个格罗布纳基.

⊖ 这实际上是习题 7.65 中给出的既约的格罗布纳基.

7.60 求 $I=(xz, xy-z, yz-x)$的一个格罗布纳基. x^3+x+1 在 I 中吗?

7.61 求 $I=(x^2-y, y^2-x, x^2y^2-xy)$的一个格罗布纳基. x^4+x+1 在 I 中吗?

*7.62 设 I 是 $k[X]$中的一个理想，其中 k 是一个域，$k[X]$有单项式序. 试证若多项式集合$\{g_1, \cdots, g_m\}\subseteq I$ 有下述性质：对每一个非零 $f\in I$，存在某个 g_i 使得 $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$，则 $I=(g_1, \cdots, g_m)$. 由此得出结论，在格罗布纳基的定义中，没有必要假设 I 是由 $g_1, \cdots, g_m$ 生成的.

*7.63 试证下面伪码给出了理想 $I=(f_1, \cdots, f_t)$的一个既约的基 Q.

```
Input: P = [f_1,…,f_t]
Output: Q = [q_1,…,q_s]
Q := P
WHILE there is q ∈ Q which is
        not reduced mod Q − {q} DO
select q ∈ Q which is not reduced mod Q − {q}
Q := Q − {q}
h := the remainder of q mod Q
IF h ≠ 0 THEN
        Q := Q ∪ {h}
   END IF
END WIHLE
make all q ∈ Q monic
```

7.64 若 G 是理想 I 的一个格罗布纳基，Q 是由习题 7.63 中的算法而得的 I 的一个基. 试证 Q 也是 I 的一个
580 格罗布纳基.

*7.65 试证下面伪码将一个格罗布纳基 G 替换成了一个既约的格罗布纳基 H.

```
Input: G = {g_1,…,g_m}
Output: H
H := ∅;   F := G
WHILE F ≠ ∅ DO
  select f′ from F
  F := F − {f′}
  IF LT(f) ∤ LT(f′) for all f ∈ F AND
       LT(h) ∤ LT(f′) for all h ∈ H THEN
     H := H ∪ {f′}
  END IF
END WHILE
```

581 对 H 应用习题 7.63 中的算法.

附录A 不 等 式

我们来证明一些实数不等式的基本性质，这样我们先给出正实数集 P 的一些性质.

(i) P 在加法和乘法下封闭，即若 a，b 在 P 中，则 $a+b$ 在 P 中且 ab 在 P 中.

(ii) **三分法**成立：若 a 是一个实数，则下列恰好有一个成立：

$$a \text{ 在 } P \text{ 中}; a = 0; -a \text{ 在 } P \text{ 中}.$$

定义 对任意两个实数 a 和 A，定义 $a<A$(也可以记为 $A>a$)表示 $A-a$ 在 P 中. 我们记 $a\leqslant A$ 表示 $a<A$ 或 $a=A$.

命题 A.1 对所有的 a，b，$c\in\mathbb{R}$，

(i) $a\leqslant a$；

(ii) 若 $a\leqslant b$ 且 $b\leqslant c$，则 $a\leqslant c$；

(iii) 若 $a\leqslant b$ 且 $b\leqslant a$，则 $a=b$；

(iv) 或者 $a<b$，或者 $a=b$，或者 $b<a$.

证明 (i) 我们有 $a\leqslant a$，因为 $a-a=0$.

(ii) 若 $a\leqslant b$，则 $b-a$ 在 P 中或者 $b=a$. 若 $b\leqslant c$，则 $c-b$ 在 P 中或者 $c=b$. 这样存在四种情况. 若 $b-a$ 在 P 中且 $c-b$ 在 P 中，则 $(b-a)+(c-b)=c-a$ 在 P 中，故 $a\leqslant c$. 若 $b-a$ 在 P 中且 $c=b$，则 $c-a$ 在 P 中，从而 $a\leqslant c$. 其他两种情况类似可得.

(iii) 假设 $a\leqslant b$ 和 $b\leqslant a$. 像在(i)中一样，存在四种情况. 若 $b-a$ 在 P 中且 $a-b$ 在 P 中，则 $(b-a)+(a-b)=0$ 在 P 中，矛盾，所以这种情况不会出现. 若 $b-a$ 在 P 中且 $b=a$，则 $b-a=b-b=0$ 在 P 中，另一个矛盾. 类似地，$a-b$ 在 P 中且 $a=b$ 这种情况也不会出现. 剩下的可能性只有 $a=b$. A-1

(iv) 由三分法，或者 $a-b$ 在 P 中，或者 $a-b=0$，或者 $-(a-b)=b-a$ 在 P 中，即或者 $a\leqslant b$，或者 $a=b$，或者 $b\leqslant a$. ■

注意，若 $a<b$ 且 $b<c$，则 $a<c$ [这是因为，$c-a=(c-b)+(b-a)$] 是 P 中两个数的和，于是 $c-a$ 在 P 中]. 通常将这两个不等式缩写为 $a<b<c$. 读者可以验证，若 $a\leqslant b\leqslant c$，则 $a\leqslant c$，而若 $a\leqslant b$ 或 $b\leqslant c$ 是严格不等式，则有 $a<c$.

命题 A.2 假设 b 和 B 是满足 $b<B$ 的实数.

(i) 若 m 是正的，则 $mb<mB$. 若 m 是负的，则 $mb>mB$.

(ii) 对任意数 N，无论是正的、负的还是零，我们有

$$N+b<N+B \text{ 和 } N-b>N-B.$$

(iii) 设 a 和 A 是正实数. 若 $a<A$，则 $\frac{1}{a}>\frac{1}{A}$. 且相反地，若 $\frac{1}{A}<\frac{1}{a}$，则 $A<a$.

证明 (i) 由假设，$B-b>0$. 若 $m>0$，则由正数的乘积还是正数推出 $m(B-b)=mB-mb$ 是正数，即，$mb<mB$. 若 $m<0$，则乘积 $m(B-b)=mB-mb$ 是负的，故 $mB<mb$.

(ii) 差 $(N+B)-(N+b)$ 是正的，因为它等于 $B-b$. 对于另一个不等式，$(N-b)-(N-B)=-b+B$ 是正的，因此 $N-b>N-B$.

(iii)若 $a<A$，则 $A-a$ 是正的. 因此 $\frac{1}{a}-\frac{1}{A}=\frac{A-a}{Aa}$ 是正的，因为它是正数 $A-a$ 和正数 $\frac{1}{Aa}$ 的乘积(由假设 a 和 A 是正数). 从而 $\frac{1}{a}>\frac{1}{A}$. 相反地，若 $\frac{1}{A}<\frac{1}{a}$，则由(i)有 $a=Aa\left(\frac{1}{A}\right)<Aa\left(\frac{1}{a}\right)=A$，即 $A>a$. ■

例如，因为 $2<3$，所以我们有 $-3<-2$ 和 $\frac{1}{3}<\frac{1}{2}$. 对一个公式，我们应该看一下几个特殊情形(尽管公式在这样少数几种情形成立不能证明此公式成立)，因为它可以帮助我们更好地

A-2 理解所要证明的东西.

附录B 伪　　码

一个解决问题的算法是一批指令，经过有限步骤后，这些指令给出了问题的正确答案，且在任何阶段，决不会使用户对下面步骤做的东西有疑问. 除法算律就是这种意义下的算法：人们从 a 和 b 开始，到 q 和 r 结束. 我们现在来用伪码更正式地处理算法. 伪码是可以很容易地翻译成程序语言的一般性的指令. 伪码的基本构件是赋值，循环结构和分支结构.

一个**赋值**是下述形式的指令

〈variable〉 := 〈expression〉.

此指令用出现在 variable(变量)中的储存的值，赋给右边的 expression(表达示)，此值存放在右边. 因此赋值用右边的新值替换左边的变量.

例 B.1 对于除法算律，考虑下伪码.

```
1: Input: b≥a>0
2: Output: q, r
3: q:=0;    r:=b
4: WHILE r≥a DO
5:    r:=r−a
6:    q:=q+1
7: END WHILE
```

开始两行的意思是很清楚的：第 3 行有两个赋值；给定变量 q 和 r 的初始值. 在考虑赋值 5 和 6 之前，让我们来解释一下**循环结构** WHILE…DO. 它的一般形式是 A-3

WHILE〈condition〉DO

〈action〉

这里，action(行动)表示一系列的指令. 只要条件成立，循环就重复 action，但当条件不再有效或被告知该结束了时，循环才会终止. 在上例中，从 $r=b$ 和 $q=0$ 开始. 因为 $b\geqslant a$，所以条件成立，故赋值 5 替换 $r=b$ 为 $r=b-a$. 类似地，赋值 5 替换 $q=0$ 为 $q=1$. 若 $r=b-a\geqslant 0$，此循环就用刚刚得到的 r 和 q 的新值重复此 action(行动).

此伪码不是商和剩余的存在性的证明的一个替换. 假如没有存在性的证明，而我们又要从此伪码开始，那我们必须证明两件事情：第一，循环最终一定会停止；第二，输出项 q 和 r 满足除法算律的必要的要求，即，$b=qa+r$ 和 $0\leqslant r<a$. ◀

例 B.2 另一个流行的循环结构是 REPERT，记为

REPEAT〈action〉UNTIL〈condition〉.

在 WHILE 中，condition(条件)告诉我们何时执行，而在 REPERT 中，condition(条件)告诉我们何时停止. 另一个差异是，WHILE 可能一步都不进行，因为在行动之前要检验条件. REPERT 总是至少进行一步，因为它总是在行动之后才检验条件.

例如，考虑求一个多项式 $f(x)$ 的实数根的牛顿法. 回忆到，我们从 $f(x)$ 一个根的估计值

a_0 开始，归纳地定义

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

若数列$\{a_n\}$收敛(它可能不收敛)，则它的极限是 $f(x)$的一个根. 下面的伪码是求 $f(x)=x^3+x^2-36$ 的一个实数根，误差至多是 0.0001.

```
Input: positive a
Output: a, y, y'
REPEAT
  y := a^3 + a^2 - 36
  y' := 3a + 2a
  a := a - y/y'
UNTIL y < .0001
```

A-4 ◀

例 B.3 下面是**重复结构** FOR 的一个例子，记为

FOR each k in K DO⟨action⟩.

这里，给定一个(有限)集 $K=\{k_1, \cdots, k_n\}$，action(行动)由进行 k_1 上的行动，再进行 k_2 上的，直到进行 k_n 上的行动组成.

例如，

```
FOR each n with 0≤n≤41 DO
  f := n^2 - n + 41
END FOR
```

◀

例 B.4 **分支结构**的一个例子是

IF⟨condition⟩THEN⟨action # 1⟩ELSE⟨action # 2⟩.

当此结构延伸且 condition(条件)成立时，则执行 action#1(仅一次)，但是当此结构延伸且 condition(条件)不成立，则执行 action#2(仅一次). 也可以省去 ELSE⟨action#2⟩，此时，指令为

IF⟨condition⟩THEN⟨action#1⟩ELSE do nothing. ◀

下面是一个执行欧几里得算法的伪码.

```
Input: a, b
Output: d
d := b;    s := a
WHILE s>0 DO
  rem := remainder after dividing d by s
  d := s
  s := rem
END WHILE
```

A-5

部分习题提示

1.1 (i)对. (ii)对. (iii)错. (iv)对. (v)对. (vi)对. (vii)对. (viii)错.

1.2 (ii)用归纳法证明或利用(i).

1.3 可转述为：存在整数 q_n 使得 $10^n=9q_n+1$.

1.8 和为 n^2.

1.9 和为 $1+\sum_{j=1}^{n} j!j=(n+1)!$.

1.10 (ii)一定要注意题设. 当 b 是负数时，考虑 a^3+b^3.

1.11 对角线上有 $n+1$ 个方格，两边两个三角形的面积都是 $\sum_{i=1}^{n} i$.

1.12 (i)用两种方式计算矩形的面积 R.

1.12 (ii)如图 1-3 所示，高为 $n+1$ 底为 $\sum_{i=1}^{n} i^k$ 的矩形可以分解使得阴影楼梯的面积是 $\sum_{i=1}^{n} i^{k+1}$，上面的面积是

$$1^k+(1^k+2^k)+(1^k+2^k+3^k)+\cdots+(1^k+2^k+\cdots+n^k).$$

1.12 (iii)在阿尔哈曾公式中记 $\sum_{i=1}^{n}\left(\sum_{p=1}^{i} p\right)=\frac{1}{2}\sum_{i=1}^{n} i^2+\frac{1}{2}\sum_{i=1}^{n} i$，然后根据余下部分解出 $\sum_{i=1}^{n} i^2$.

1.13 (i)在归纳步中，利用 $n\geqslant 10$ 推出 $n\geqslant 4$.

1.13 (ii)在归纳步中，利用 $n\geqslant 17$ 推出 $n\geqslant 7$.

1.14 可以假设当 $0\leqslant r<1$ 时 $\sum_{n=0}^{\infty} ar^n=a/(1-r)$.

1.15 基础步是导数的乘积法则.

1.16 不等式 $1+x>0$ 允许我们利用命题 A. 2.

1.17 模仿命题 1.14 的证明. 把“偶数”改为“3 的倍数”，把“奇数”改为“不是 3 的倍数”.

1.18 归纳法的恰当形式是如何使用的？

1.19 利用定理 1.15 以及几何级数.

1.20 对于归纳步，试着加减相同的项.

1.21 若 $2\leqslant a\leqslant n+1$，则 a 是 $a+(n+1)!$ 的一个因子. 更多的证明不使用归纳法.

1.25 利用平均不等式.

1.26 (i)利用**海伦(Heron)公式**：若三角形的面积为 A，三边长为 a，b，c，则 $A^2=s(s-a)(s-b)(s-c)$，其中 $s=\frac{1}{2}(a+b+c)$.

1.26 (ii)利用海伦公式以及平均不等式.

1.27 若 $p\geqslant q>0$，$p'\geqslant q'>0$，则 $pp'\geqslant qq'$.

1.28 (i)对. (ii)错. (iii)对. (iv)对. (v)对. (vi)错. (vii)对.

1.29 验证对实数的证明中使用的加法和乘法性质对复数也是成立的.

1.31 当 $x=1$ 时，考虑 $f(x)=(1+x)^n$.

1.32 (i)当 $x=-1$ 时，考虑 $f(x)=(1+x)^n$.

1.33 取 $f(x)=(1+x)^n$ 的导数.

1.35 (i)利用三角不等式以及对 n 用归纳法.

1.35 (ii)利用下列点积的性质：若 $u, v\in\mathbb{C}$，则 $|u|^2=u\cdot u$，$u\cdot v=|u|\,|v|\cos\theta$，其中 θ 是 u 和 v 的夹角.

1.37 只有 i 的奇次幂可以想到.

1.38 (ii)与(i)作比较.

1.40 5 个数的选择有多少种？

1.42 即使非常相似，也没有常规的方法由二项式定理导出莱布尼茨公式(有一种方法是利用超几何级数来导出).

1.45 (i)(8, 15)的极坐标是(17, 62°)，并且 $\sin 31°\approx 0.515$，$\cos 31°\approx 0.857$.

1.45 (ii)$\sin 15.5°\approx 0.267$，$\cos 15.5°\approx 0.967$.

H-2 **1.46** (i)错. (ii)对. (iii)对. (iv)错. (v)对. (vi)对. (vii)错. (viii)对. (ix)对. (x)错.

1.47 利用完全除法算式中已经证明的那部分.

1.49 $19\mid f_7$，但 7 不是最小的 k.

1.51 利用推论 1.37.

1.52 把 m 写成以 2 为底数的表达式.

1.54 (i)假设 $\sqrt{n}=a/b$，其中 a/b 是既约形式，并改写命题 1.43 的证明.

1.54 (ii)假设可把 $\sqrt[3]{2}$ 写为既约分数.

1.58 若 $ar+bm=1$，$sr'+tm=1$，则考虑 $(ar+bm)(sr'+tm)$.

1.59 若 $2s+3t=1$，则 $2(s+3)+3(t-2)=1$.

1.60 利用推论 1.40.

1.61 若 $b\geqslant a$，则 a 和 b 的公因子也是 a 和 $b-a$ 的公因子.

1.62 证明：若 k 是 ab 和 ac 的公因子，则 $k\mid a(b, c)$.

1.64 利用辗转相除法中的思想.

1.68 (i)错. (ii)对. (iii)对. (iv)对. (v)对.

1.70 (ii)利用推论 1.53.

1.71 a 和 b 的所有素因子构成的集合是不相交的.

1.72 运用反证法并使用欧几里得引理.

1.76 (i)设 a 和 b 都不等于 0，证明 $ab/(a, b)$ 是 a 和 b 的公倍数且能整除 a 和 b 的任意公倍数 c.

1.77 (i)对. (ii)错. (iii)错. (iv)错. (v)错. (vi)错. (vii)对. (viii)错.

1.79 弃 9 法.

1.80 $10\equiv -1 \bmod 11$.

1.81 $100=2\cdot 49+2$.

1.85 利用例 1.61 中的一个结论：若 a 是一个完全平方数，则 $a^2\equiv 0, 1, 4 \bmod 8$.

1.86 若 a^2 的最后一位数字是 5，则 $a^2\equiv 5 \bmod 10$. 若 a^2 的最后两位数字是 35，则 $a^2\equiv 35 \bmod 100$.

H-3 **1.88** 利用欧几里得引理.

1.90 根据习题 1.60，我们有 $21\mid(x^2-1)$ 当且仅当 $3\mid(x^2-1)$，$7\mid(x^2-1)$.

1.92 利用中国剩余定理的证明. 答案是 199.

1.94 (i)考虑 a 和 b 的奇偶性.

1.97 4 个椰子.

1.98 复活节总是在星期日.（犹太人对这个问题的提法不同，因为赎罪日一定是星期一、星期三、星期四或星期六中的某一天；非宗教的节日可以包含感恩节，它总是在某个星期四，或选举日，选举日总是在某个星期四.）

1.99 $y=1900$ 年不是闰年.

1.100 1896 年 3 月 1 日是星期几?

1.101 (iii)利用同余或浏览 14 个可能的日历：有 7 个平年和 7 个闰年，因为 1 月 1 日可以是一个星期中的任何一天.

1.102 在美国 1900 年不是闰年.

2.1 (i)对. (ii)错. (iii)对. (iv)对. (v)对. (vi)错. (vii)错. (viii)错. (ix)对.

2.4 (iv)证明图 2-7 描述了 $A+(B+C)$和$(A+B)+C$.

2.5 约束关系$\in$的公理之一是：命题

$$a \in x \in a$$

恒不成立.

2.6 (i)可以利用这些事实：(1)斜率分别为 m_1 和 m_2 的直线 ℓ_1 和 ℓ_2 垂直当且仅当 $m_2m_2=-1$；(2)端点为(a, b)和(c, d)的线段的中点是$\left(\frac{1}{2}(a+c), \frac{1}{2}(b+d)\right)$.

2.7 (i)利用命题 2.2.

2.8 g 有反函数吗?

2.10 证明 f 有一个反函数，或者证明 f 是单射且是满射.

2.11 不是.

2.12 若 f 是一个双射，则 Y 中有 m 个不同的元素 $f(x_1), \cdots, f(x_m)$，因此 $m\leqslant n$. 再利用双射 f^{-1} 给出反不等式 $n\leqslant m$.

2.13 (i)若 $A\subseteq X$, $|A|=n=|X|$，则 $A=X$. 毕竟，有多少个元素在 X 中但不在 A 中? H-4

2.15 (i)计算合成运算.

2.20 (i)y 是什么?

2.21 (i)错. (ii)对. (iii)对. (iv)错. (v)错. (vi)对. (vii)错. (viii)对. (ix)错. (x)错.

2.23 利用 σ 和σ' 的完全因子分解.

2.24 (i)任意 r-循环置换都有 r 个循环记号.

2.25 (i)设 $\alpha=(i_0\cdots i_{r-1})$，证明对 $k<r$ 有 $\alpha^k(i_0)=i_k$.

2.25 (ii)利用命题 2.24.

2.27 对 $j-i$ 用归纳法.

2.29 (i)设 $\alpha=(a_1\ a_2\cdots a_k)(b_1\ b_2\cdots\ b_k)\cdots(c_1\ c_2\cdots c_k)$是不相交的 k-循环置换的乘积，证明 $\alpha=\beta^k$，其中$\beta=(a_1\ b_1\cdots z_1\ a_2\ b_2\cdots\ z_2\cdots\ a_k\ b_k\cdots\ z_k)$.

2.30 (i)首先对 k 用归纳法证明 $\beta\alpha^k=\alpha^k\beta$.

2.32 设 $\tau=(1\ 2)$，定义 $f: A_n\to O_n$, $f: \alpha\mapsto\tau\alpha$，其中 A_n是所有偶置换构成的集合，O_n是所有奇置换构成的集合. 证明 f 是一个双射，从而 $|A_n|=|O_n|$.

2.35 不能.

2.36 (i)错. (ii)错. (iii)对. (iv)错. (v)错. (vi)对. (vii)错. (viii)错. (ix)错. (x)对.

2.39 (i)在 S_5 中阶为 2 的元素有 25 个，在 S_6 中阶为 2 的元素有 75 个.

2.39 (ii)可以把答案表示成一个和，非封闭式的.

2.40 显然$(y^i)^d=1$，利用引理 2.53 证明没有 y^i的更小的幂等于 1.

2.43 (i)对 $k\geqslant1$ 用归纳法.

2.45 考虑由 $f(x)=x^2$定义的函数 $f: G\to G$.

2.46 把每个元素与它的逆元配对.

2.47 对任意 n，没有一般公式.

2.52 (i)对. (ii)对. (iii)错. (iv)错. (v)对. (vi)错. (vii)对. (viii)错. (ix)对. (x)对. (xi)错

H-5

2.55 设 G 是四元群 **V**.

2.57 考虑 $|H\cap K|$.

2.58 一个无限群能否只有有限个循环子群?

2.61 设 $G\neq ST$，找 G 的两个不相交的子群，且它们分别有 $|S|$ 和 $|T|$ 个元素.

2.62 (ii)对不同子群 S_i 的个数运用归纳法证明.

2.63 (ii)考虑 $aH\mapsto Ha^{-1}$.

2.64 (i)对. (ii)错. (iii)对. (iv)对. (v)错. (vi)对. (vii)错. (viii)对. (ix)对. (x)对.

2.65 若 $\alpha\in S_X$，则定义 $\varphi(\alpha)=f\circ\alpha\circ f^{-1}$. 特别地，证明：若 $|X|=3$，则 φ 把含 1，2，3 的循环置换映射到含 a，b，c 的循环置换，和例 2.88 一样.

2.75 利用共轭.

2.77 (i)考虑 φ：$A=\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}\mapsto(\cos\alpha,\ \sin\alpha)$.

2.78 列举素数 $p_0=2$，$p_1=3$，$p_2=5$，…，并定义

$$\varphi(e_0+e_1x+e_2x^2+\cdots+e_nx^n)=p_0^{e_0}\cdots p_n^{e_n}.$$

2.82 证明乘方是一个单射函数 $G\to G$，并利用习题 2.13.

2.83 取 $G=S_3$，$H=\langle(1\ 2)\rangle$，$g=(2\ 3)$.

2.84 证明，若 A 是一个矩阵且非数量矩阵，则存在非奇异矩阵与 A 不交换(对 $n\times n$ 矩阵的这一证明在命题 4.86 中给出).

2.85 (iii)考虑情形 A^iA^j，A^iBA^j，BA^iA^j，$(BA^i)(BA^j)$.

2.86 (i)注意 $A^2=-I=B^2$.

2.87 利用习题 2.69.

2.89 (ii)利用命题 2.97(ii).

2.90 (iii)见例 2.48(iv).

H-6

2.91 π_n 的顶点集合 $X=\{v_0,\ \cdots,\ v_{n-1}\}$ 被每个等距 $\varphi\in\Sigma(\pi_n)$ 所置换.

2.95 (i)错. (ii)错. (iii)对. (iv)对. (v)错. (vi)对. (vii)对. (viii)错. (ix)错. (x)对.

2.97 (iii)定义 f：$H\times K\to H$，$f:(h,\ k)\mapsto h$.

2.98 若 $G/Z(G)$ 是循环群，则利用一个生成元构造一个元素，它不属于 $Z(G)$ 但与 G 的每个元素交换.

2.99 $|G|=|G/H|\ |H|$.

2.100 对 $n\geqslant 1$ 运用归纳法，其中 $X=\{a_1,\ \cdots,\ a_n\}$. 归纳步应该考虑商群 $G/\langle a_{n+1}\rangle$.

2.105 若 $H\leqslant G$，则 $|H|=|K|$，G/K 中 H 的元素怎么了?

2.106 (i)利用结论 $H\subseteq HK$，$K\subseteq HK$.

2.111 (ii)利用习题 2.110.

2.112 利用威尔逊定理.

2.114 (i)错. (ii)对. (iii)错. (iv)错. (v)错. (vi)错. (vii)对. (viii)对. (ix)错. (x)对. (xi)对. (xii)错. (xiii)对. (xiv)错.

2.117 利用柯西定理.

2.120 利用命题 2.135.

2.121 (i)回忆 A_4 没有阶为 6 的元素.

2.121 (ii)每个元素 $x \in D_{12}$ 都有唯一因子分解 $x = b^i a$，其中 $b^6 = 1$，$a^2 = 1$.

2.122 (ii)使用第二同构定理.

2.123 可以使用如下结论：阶为 8 的非阿贝尔群只有 D_8 和 **Q**.

2.124 (i)S_4 中有 8 个置换可以与(1 2)(3 4)交换，其中 4 个是偶置换.

2.125 (i)设 $\alpha = (1\ 2\ 3\ 4\ 5)$，因为 $24 = 120/|C_{S_5}(\alpha)|$，所以 $|C_{S_5}(\alpha)| = 5$，因此 $C_{S_5}(\alpha) = \langle\alpha\rangle$. $C_{A_5}(\alpha)$是什么？

2.127 (i)像引理 2.155 的证明一样，证明(1 2 3)和$(i\ j\ k)$是共轭的.

2.129 利用命题 2.33 检查各种各样的循环结构，一次检查一个.

2.131 利用命题 2.97(ii).

2.133 (i)核是正规子群.

2.133 (ii)利用(i). H-7

2.134 证明 G 有一个阶为 p 的子群 H，并利用在 H 的陪集上 G 的表示.

2.135 假设 H 是第二个这样的子群，则 H 在 S_n中是正规的，因此 $H \cap A_n$在 A_n中是正规的.

2.137 (i)错. (ii)错. (iii)错. (iv)对. (v)对. (vi)对.

2.138 与 n 的奇偶性有关.

2.141 (i)群 $G = D_{10}$在作用. 利用例 2.64 给每个对称分配顶点的一个置换，然后证明

$$P_G(x_1, \cdots, x_5) = \frac{1}{10}(x_1^5 + 4x_5 + 5x_1 x_2^2)$$

和

$$P_G(q, \cdots, q) = \frac{1}{10}(q^5 + 4q + 5q^3).$$

2.141 (ii)群 $G = D_{12}$在作用. 利用例 2.64 给每个对称分配顶点的一个置换，然后证明

$$P_G(x_1, \cdots, x_6) = \frac{1}{12}(x_1^6 + 2x_6 + 2x_3^2 + 3x_2^2 + 4x_2^3)$$

和

$$P_G(q, \cdots, q) = \frac{1}{12}(q^6 + 2q + 5q^2 + 4q^3).$$

3.1 (i)错. (ii)对. (iii)错. (iv)对. (v)对. (vi)错. (vii)错. (viii)对.

3.7 (i)可以利用集合论的一些标准事实：

$$U \cap (V \cup W) = (U \cap V) \cup (U \cap W);$$

若 V' 表示 V 的补集，则

$$U - V = U \cap V';$$

摩根律(习题 2.3)：

$$(U \cap V)' = U' \cup V', \qquad (U \cup V)' = U' \cap V'.$$

3.11 (i)若 $zw = 0$ 且 $z = a + ib \neq 0$，则 $z\bar{z} = a^2 + b^2 \neq 0$ 且

$$\left(\frac{\bar{z}}{z\bar{z}}\right)z = 1.$$

3.13 **Z** 的每个子群 R 都含有 1.

3.14 利用定理 1.69. H-8

3.15 (i)是.

3.15 (ii)不是.

3.17 (i)对. (ii)对. (iii)错. (iv)错. (v)对. (vi)对. (vii)错.

3.20 设 $R^{\times}$ 是 R 的所有非零元素构成的集合，证明用 r 乘是一个单射 $R^{\times} \to R^{\times}$，其中$r \in R^{\times}$.

3.21 利用推论 1.23.

3.28 (i)见例 2.48(iv).

3.29 (i)对. (ii)对. (iii)错. (iv)对. (v)对. (vi)对. (vii)错.

3.30 若 x^{-1}存在，则它的次数是多少?

3.32 (i)计算次数.

3.33 利用费马定理.

3.34 (i)在 $\mathbb{F}_p[x]$ 中比较$(1+x)^{pm}$和$(1+x^m)^p$的二项展开式.

3.36 这个习题不难但证明很长.

3.38 (ii)条件是：存在一个多项式 $g(x)=\sum a_n x^n$满足 $f(x)=g(x^p)$，即 $f(x)=\sum b_n x^{np}$，其中对所有 n 有 $b_n^p=a_n$.

3.39 (i)命题 3.25 中对多项式的证明在这里也适用.

3.40 (i)设 R 是整环，σ，$\tau \in R[[x]]$ 是非零的，证明 $\operatorname{ord}(\sigma\tau)=\operatorname{ord}(\sigma)+\operatorname{ord}(\tau)$，因此 $\sigma\tau$ 有一个阶.

3.41 (i)对. (ii)错. (iii)错. (iv)对. (v)错. (vi)错. (vii)对. (viii)对. (ix)对. (x)对.

3.43 (ii)首先证明 $1+1=0$，接着证明非零元素在乘法下形成一个阶为 3 的循环群.

3.48 利用前面的习题去证明 φ 是一个同态.

3.51 (i)定义 Φ：$\operatorname{Frac}(A) \to \operatorname{Frac}(R)$，$[a, b] \mapsto [\varphi(a), \varphi(b)]$.

3.54 (i)证明(r, s)是 $R \times S$ 中的单元当且仅当 r 是 R 中的单位且 s 是 S 中的单位.

3.54 (ii)见定理 2.128.

3.55 (ii)由 $\varphi(A)=a+ib$ 定义 φ：$F \to \mathbb{C}$.

3.56 (i)对. (ii)错. (iii)错. (iv)对. (v)错. (vi)对. (vii)对. (viii)对. (ix)对. (x)对.

H-9 **3.57** (ii)利用推论 3.52.

3.58 答案是 $x-2$

3.60 利用 $\operatorname{Frac}(R)$.

3.63 利用 $\operatorname{Frac}(R)$.

3.64 见习题 1.58.

3.66 模仿命题 1.43 中对 $\sqrt{2}$ 是无理数的证明.

3.67 利用习题 3.37.

3.69 (ii)一般的证明可以从多项式这一特殊情形的证明中推广得到.

3.71 存在 q，$r \in R$ 可使 $b^i = qb^{i+1}+r$.

3.72 利用习题 3.40.

3.73 (i)例 3.39.

3.74 利用习题 1.76.

3.77 见命题 1.34.

3.78 (i)利用一个关于次数的命题.

3.79 证明 $\sqrt{x}+1$ 不是多项式.

3.81 设 k 是一个域，R 是由所有不含线性项的多项式构成的 $k[x]$ 的子环；即 $f(x) \in R$ 当且仅当

$$f(x) = s_0 + s_2 x^2 + s_3 x^3 + \cdots.$$

证明 x^5 和 x^6 没有最大公因子.

3.82 (i)错. (ii)对. (iii)错. (iv)对. (v)错. (vi)对.

3.84 (i)见习题 3.67 和推论 3.75.

3.85 (i)利用定理 3.50.

3.85 (ii)令 $x=a/b$，其中 $b\neq 0$.

3.86 (i)对. (ii)错. (iii)对. (iv)错. (v)对. (vi)错. (vii)错. (viii)对. (ix)错. (x)对. (xi)错. (xii)对. (xiii)错. (xiv)对.

3.87 (i)不可约. (ii)、(iii)不可约. (iv)不可约. (v)不可约. (vi)不可约. (vii)不可约. 证明 $f(x)$在$\mathbb{Q}$中没有根，且 $f(x)$分解成二次多项式的积时会迫使对系数有一些不可能的限制. (viii)不可约. 证明 $f(x)$没有有理根，且 $f(x)$分解成二次多项式的积时会迫使对系数有一些不可能的限制. (ix)不可约. (x)不可约. H-10

3.89 $\mathbb{F}_2[x]$ 中不可约的五次多项式是：

$$x^5+x^3+x^2+x+1 \qquad x^5+x^4+x^2+x+1$$
$$x^5+x^4+x^3+x+1 \qquad x^5+x^4+x^3+x^2+1$$
$$x^5+x^3+1 \qquad x^5+x^2+1$$

3.90 (i)利用艾森斯坦因准则.

3.91 $f(x)\mapsto f^*(x)$将系数倒过来，它不是定义良好的函数 $k[x]\to k[x]$.

3.92 (i)对. (ii)对. (iii)对. (iv)错. (v)错. (vi)对. (vii)对. (viii)对. (ix)错. (x)错. (xi)对. (xii)对. (xiii)错. (xiv)对. (xv)对.

3.94 (i)改写定理 1.73 的证明即可.

3.94 (ii)见定理 2.128 的证明.

3.95 见习题 3.84.

3.97 (i)利用习题 2.13.

3.98 利用习题 2.61.

3.99 证明$\mathbb{F}_p^\times \cong \langle -1\rangle \times H$，其中 H 是阶为奇数 m 的群，观察到 2 或 -2 在 H 中，因为

$$\mathbb{F}_2 \times \mathbb{I}_m = (\{1\}\times H)\cup(\{-1\}\times H).$$

最后，利用习题 2.82.

3.100 (ii)在扩张右边之后，像系数一样视为相等.

3.100 (iii)在第一种情形中，令 $a=0$ 并利用 b 分解 x^4+1. 若 $a\neq 0$，则 $d=b$ 和 $b^2=1$(所以 $b=\pm 1$)；现在利用 a 分解 x^4+1.

3.100 (iv)利用习题 3.99.

3.103 参见例 4.127.

3.104 (ii)利用含 p^n个元素的域的存在性.

3.105 若 E 的特征为 p，则 E 中每个非零元素的阶为 p.

4.1 (i)对. (ii)对. (iii)错. (iv)错. (v)对. (vi)对. (vii)错. (viii)错. (ix)对. (x)对.

4.4 若 u，$v\in V$，用两种方法计算 $-[(-v)+(-u)]$.

4.8 (i)两个多项式什么情况下相等？ H-11

4.9 向量 $v=(a, b)$的斜率是 $m=b/a$.

4.10 (ii)利用$\mathbb{R}^3$中的坐标重写向量 u，v 和 n.

4.12 (ii)若 A 是斜对称，则其对角线上的表值都是 0.

4.13 利用定理 3.83.

4.14 证明，对所有 i，j 有 $(e_i, e_j)=\delta_{ij}$，其中 δ_{ij} 是克罗内克 δ 函数.

4.15 给定 A，证明存在 m 使得 I，A，A^2，…，A^m 是线性无关的.

4.17 证明，若 v_1+U，…，v_r+U 是 V/U 的一个基，则 v_1，…，v_r 是线性无关的.

4.19 (ii)取 $U\cap U'$ 的一个基并将它扩充为 U 的基和 U' 的基.

4.23 (i)错. (ii)对. (iii)错. (iv)对. (v)对. (vi)对.

4.24 (ii)设 A 是一个矩阵，其行是给定的向量，看是否有 $\text{rank}(A)=m$.

4.25 若 A 是行为 v_1，v_2，v_3 的矩阵，则 $\text{rank}(A)=3$ 吗?

4.27 若 $\gamma\in k^m$，证明 $A\gamma$ 是 A 的列的一个线性组合.

4.29 (ii)设 A 是与梯形矩阵 U 高斯等价的矩阵，使得存在非奇异矩阵 P 满足 $PA=U$. 证明 β 位于行空间 $\text{Row}(A)$ 当且仅当 $P\beta\in\text{Row}(U)$.

4.30 (ii)若 $E_p\cdots E_1A=I$，则 $A^{-1}=E_1^{-1}\cdots E_p^{-1}$. 由此知，把 A 变为 I 的初等行变换也把 I 变成 A^{-1}. 答案是

$$A^{-1}=\frac{1}{4}\begin{bmatrix}1 & -3 & -1\\ 1 & 1 & -1\\ -1 & 3 & 5\end{bmatrix}$$

4.31 (ii)利用推论 4.40.

4.32 (i)错. (ii)错. (iii)对. (iv)错. (v)对. (vi)对. (vii)对. (viii)错. (ix)对. (x)对.

4.38 (ii)以下是命题. 若 f: $V\to W$ 是满足 $\ker f=U$ 的一个线性变换，则 U 是 V 的一个子空间且存在一个同构 φ: $V/U\to\text{im}f$，即 $\varphi(v+U)=f(v)$.

4.40 利用定理 4.62.

H-12 **4.46** (i)错. (ii)对. (iii)错. (iv)错. (v)错. (vi)对. (vii)错. (viii)对. (ix)错. (x)对.

4.49 看初等行变换.

4.52 (ii)$0=1-\omega^n=(1-\omega)(1+\omega+\omega^2+\cdots+\omega^{n-1})$.

4.54 (i)定义 $T^{\#}(e_i)=\overline{a}_{1i}e_1+\cdots+\overline{a}_{ni}e_n$.

4.54 (iv)采用定理 4.104 的证明.

4.60 若对所有 i 有 $B_i=P_iA_iP_i^{-1}$，则 $(P_1\oplus\cdots\oplus P_t)^{-1}=P_1^{-1}\oplus\cdots\oplus P_t^{-1}$.

4.62 首先假设 $c\in k$.

4.65 回忆幂级数 $1/x=1-x+x^2-x^3+\cdots$，其中 x 是一个非零实数.

4.70 C 是无交并 $\bigcup_{c\in C}B_1(c)$.

4.73 若 $C=\{(a, a)\in\mathbf{F}^2\}$，则 C 纠正了 1 个错误. 若 $w=(a, b)$，其中 $a\neq b$，则 $w\notin C$ 且 $\delta(w, (a, a))=1=\delta(w, (b, b))$.

4.76 (i)利用 $\mathbb{Z}[x]$ 中的分解式 $x^{15}-1=\Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)$，其中 $\Phi_d(x)$ 是 d 次分圆多项式.

4.76 (ii)尝试 $g(x)=x^4+x+1$.

4.76 (iii)证明 ζ^2 是 $g(x)$ 的一个根.

4.77 利用例 4.127 中的表 4-1. 答案是

$$c=(\zeta^3,\zeta,1+\zeta^3,\zeta^3+\zeta,0,\zeta^3,1).$$

5.1 (ii)给定 $\mathbb{Q}[x]$ 中的一个首一多项式，我们应当首先利用定理 3.90 看出它是否有有理(一定是整数)根.

5.6 对方程 $f(u)=0$ 应用复共轭.

5.8 $r=\cos 3\theta=\cos 3(\theta+120°)=\cos 3(\theta+240°)$.

5.9 (i)由定义知 $\cosh\theta=\frac{1}{2}(e^{\theta}+e^{-\theta})$. 将它推广然后简化

$$4\left[\frac{1}{2}(e^{\theta}+e^{-\theta})\right]^3-3\left[\frac{1}{2}(e^{\theta}+e^{-\theta})\right]$$

得到 $\frac{1}{2}(e^{3\theta}+e^{-3\theta})$.

5.9 (ii)由定义知 $\sinh\theta=\frac{1}{2}(e^{\theta}-e^{-\theta})$.

5.10 根是 -4 和 $2\pm\sqrt{-3}$.

5.11 根是 17 和 $\frac{1}{2}(-1\pm\sqrt{-3})$.

5.12 (i)根以不可认识的形式出现.

5.12 (ii)根是 4 和 $-2\pm\sqrt{3}$. H-13

5.13 根是 2 和 $-1\pm\sqrt{3}$.

5.14 这是一个很麻烦的计算，根是 -3，-1，$2\pm\sqrt{6}$.

5.15 (i)错. (ii)错. (iii)错. (iv)错. (v)错. (vi)对. (vii)错. (viii)对. (ix)错.

5.20 不是.

5.21 (ii)利用命题 1.39.

5.21 (iii)利用习题 2.13，证明当 k 有限时弗罗贝尼乌斯函数 $F: k\to k$ 是满射.

5.22 (ii)利用命题 3.116.

5.22 (iii)证明，若 $\sigma\in G$，则 σ 完全由 $\sigma(\alpha)$ 确定，它是 α 的不可约多项式的一个根.

5.22 (iv)证明 F 的阶 $\geqslant n$.

5.25 观察到 $\mathbb{F}_5[x]$ 中有 $x^{30}-1=(x^6-1)^5$.

5.29 (i)若 α 是 $f(x)$ 的一个实根，则 $\mathbb{Q}(\alpha)$ 不是 $f(x)$ 的分裂域.

5.29 (ii)利用(i).

5.29 (iii)尝试 $g(x)=3x^3-3x+1$.

5.30 (ii)利用习题 3.67.

5.32 (i)考虑 $f(x)=x^p-t\in\mathbb{F}_p(t)[x]$.

6.1 (i)错. (ii)错. (iii)对. (iv)对. (v)对. (vi)错. (vii)错. (viii)错. (ix)错. (x)对.

6.6 (ii)利用(i).

6.6 (iii)利用(i).

6.8 有 14 个群.

6.10 若 B 是阶为 p^n 的循环群的 k 次直和，则 B 中有多少个阶为 p^n 的元素?

6.11 (iii)若 A 和 B 都是 $\mathbb{Q}$ 的非零子群，则 $A\cap B\neq\{0\}$.

6.12 (i)利用基定理(定理 6.11)的证明.

6.13 若 F 是 m 个无限循环群的直和，证明 $F/2F$ 是 $\mathbb{F}_2$ 上一个 m 维向量空间.

6.20 (i)错. (ii)对. (iii)对. (iv)对. (v)错. (vi)对. (vii)错. (viii)对. (ix)错. (x)对. H-14

6.22 考虑 $S_3\times S_3$.

6.24 若 $g\in G$，则 gPg^{-1} 是 K 的一个西罗 p-子群，所以它在 K 中与 P 共轭.

6.25 看习题 3.28.

6.26 只需求出 S_6 的阶为 16 的一个子群. 考虑无交并 $\{1, 2, 3, 4, 5, 6\}=\{1, 2, 3, 4\}\cup\{5, 6\}$ 并利用习题 2.106.

6.27 利用 G 的任意西罗 p-子群与 P 共轭这个事实.

6.28 计算由西罗子群生成的子群的阶.

6.29 (i)证明 p 既不整除 $[G/H: HP/H]$ 也不整除 $[H: H\cap P]$.

6.29 (ii)选取 S_4 的一个子群 H 满足 $H\cong S_3$，并求出 S_4 的满足 $H\cap P=\{1\}$ 的一个子群 P.

6.31 有一些不是很难.

6.32 应用准素分解的证明.

6.34 由柯西定理知，G 一定含有阶为 p 的元素 a，且 $\langle a\rangle \lhd G$，因为它的指数是 2.

6.35 (i)每个独立的子集可以扩充为一个基.

6.35 (ii)群 $GL(r, k)$ 在由 $(\mathbb{F}_q)^n$ 中所有线性无关的 r 序列构成的集合 X 上作用，并利用定理 6.30 的证明.

6.38 (i)利用行列式.

6.38 (ii)利用(i)和定理 6.30.

6.38 (iii)证明矩阵 $A=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ 和 $B=\begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}$ 生成一个阶为 8 的子群，它与 $\mathbf{Q}$ 同构.

6.39 (i)错. (ii)错. (iii)错. (iv)错. (v)对. (vi)错. (vii)对. (viii)对.

6.48 (i)设 $\rho(z)=e^{i\theta}\bar{z}$，定义 $R(z)=e^{i\alpha}z$，其中 $\alpha=\frac{1}{2}(2\pi-\theta)$.

6.51 证明每个 $g\in G$ 有唯一表示 $g=a^ib^j$，其中 $i\in\{0, 1\}$，$j\in\mathbb{Z}$.

7.1 (i)对. (ii)对. (iii)错. (iv)错. (v)对. (vi)错. (vii)错. (viii)对. (ix)对. (x)对.

7.3 什么时候布尔环是一个整环?

H-15 **7.5** (ii)设 $f: \mathbb{Z}\to \mathbb{I}_4$ 是一个自然映射，并取 $Q=\{0\}$.

7.15 (ii)对于满射性，若 I，J 互素，则存在 $a\in I$，$b\in J$ 使得 $I=a+b$. 设 r，$r'\in R$，证明 $(d+I, d+J)=(r+I, r'+J)\in R/I\times R/J$，其中 $d=r'a+rb$.

7.16 (iii)可以假设在交换环中每个非单位位于某个极大理想中(可以利用佐恩引理证明该结论).

7.17 (i)对. (ii)对. (iii)对. (iv)错. (v)错. (vi)对. (vii)错. (viii)错. (ix)对. (x)对.

7.29 (i)错. (ii)错. (iii)对. (iv)错. (v)错. (vi)错. (vii)对. (viii)对.

7.35 利用习题 1.2(i).

7.36 设 $f^r\in I$，$g^s\in I$，证明 $(f+g)^{r+s}\in I$.

参考文献

Albert, A. A., *Introduction to Algebraic Theories*, University of Chicago Press, 1941.

Artin, M., *Algebra*, Prentice Hall, Upper Saddle River, NJ, 1991.

Baker, A., *Transcendental Number Theory*, Cambridge University Press, 1979.

Becker, T., and Weispfenning, V., *Gröbner Bases: a Computational Approach to Commutative Algebra*, Springer-Verlag, New York, 1993.

Berlekamp, E. R., Conway, J. H., and Guy, R. K., *Winning Ways for Your Mathematical Plays*, Academic Press, Orlando, FL, 1982.

Biggs, N. L., *Discrete Mathematics*, Oxford University Press, 1989.

Birkhoff, G., and Mac Lane, S., *A Survey of Modern Algebra*, 4th ed., Macmillan, New York, 1977.

Blake, I. F., and Mullin, R. C., *The Mathematical Theory of Coding*, Academic Press, New York, 1975.

Burn, R. P., *Groups: A Path to Geometry*, Cambridge University Press, Cambridge, 1985.

Burnside, W., *The Theory of Groups of Finite Order*, Cambridge University Press, 1911.

Cajori, F., *A History of Mathematical Notation*, Open Court, 1928; Dover reprint, 1993.

Carmichael, R., *An Introduction to the Theory of Groups of Finite Order*, Ginn, Boston, 1937.

Cox, D., Little, J., and O'Shea, D., *Ideals, Varieties, and Algorithms*, 3d ed., Springer-Verlag, New York, 1992.

Curtis, C., *Linear Algebra; An Introductory Approach*, Springer-Verlag, New York, 1984.

Dornhoff, L. L., and Hohn, F. E., *Applied Modern Algebra*, Macmillan, New York, 1978.

Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995.

Fröhlich, A., and Taylor, M. J., *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991.

Gorenstein, D., Lyons, R., and Solomon, R., *The Classification of the Finite Simple Groups*, Math. Surveys and Monographs, Volume 40, American Mathematical Society, Providence, 1994.

Hadlock, C., *Field Theory and its Classical Problems*, Carus Mathematical Monographs No. 19, Mathematical Association of America, Washington, 1978.

Herstein, I. N., *Topics in Algebra*, 2d ed., Wiley, New York, 1975.

Hoffman, D. G., Leonard, D. A., Lindner, C. C., Phelps, K. T., Rodger, C. A., and Wall, J. R., *Coding Theory: The Essentials*, Marcel Dekker, New York, 1991.

Jacobson, N., *Basic Algebra* I, Freeman, San Francisco, 1974.

————, *Basic Algebra* II, Freeman, San Francisco, 1980.

Kaplansky, I., *Fields and Rings*, 2d ed., University of Chicago, 1974.

Laywine, C. F., and Mullen, G. L., *Discrete Mathematics Using Latin Squares*, Wiley, New York, 1998.

Leon, Steven J., *Linear Algebra with Applications*, 6th ed., Prentice Hall, Upper Saddle River, 2002.

Li, C. C., *An Introduction to Experimental Statistics*, McGraw-Hill, New York, 1964.

Lidl, R., and Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1986.

Ling, S., and Xing, C., *Coding Theory, A First Course*, Cambridge University Press, 2004.

Martin, G. E., *Transformation Geometry: An Introduction to Symmetry*, Springer-Verlag, New York, 1982.

McCoy, N. H., and Janusz, G. J., *Introduction to Modern Algebra*, 5th ed., Wm. C. Brown Publishers, Dubuque, 1992.

Nagpaul, S. R., and Jain, S. K., *Topics in Applied Abstract Algebra*, Brooks/Cole, Belmont, 2005.

Niven, I., and Zuckerman, H. S., *An Introduction to the Theory of Numbers*, Wiley, New York, 1972.

Pollard, H., *The Theory of Algebraic Numbers*, Carus Mathematical Monographs No. 9, Mathematical Association of America, Washington, 1950.

Rotman, J. J., *Advanced Modern Algebra*, Prentice Hall, Upper Saddle River, 2002.

———, *Galois Theory*, 2d ed., Springer-Verlag, New York, 1998.

———, *An Introduction to the Theory of Groups*, 4th ed., Springer-Verlag, New York, 1995.

———, *Journey into Mathematics*, Prentice Hall, Upper Saddle River, 1998.

Ryser, H. J., *Combinatorial Mathematics*, Carus Mathematical Monographs No.14, Mathematical Association of America, Washington, 1963.

Stark, H. M., *An Introduction to Number Theory*, Markham, Chicago, 1970.

Stillwell, J., *Mathematics and Its History*, Springer-Verlag, New York, 1989.

Suzuki, M., *Group Theory I*, Springer-Verlag, New York, 1982.

Thompson, T. M., *From Error-Correcting Codes Through Sphere Packings to Simple Groups*, Carus Mathematical Monographs No. 21, Mathematical Association of America, Washington, 1983.

Tignol, J.-P., *Galois' Theory of Equations*, World Scientific, Singapore, 1988.

Trappe, W., and Washington, L. C., *Introduction to Cryptography with Coding Theory*, Prentice Hall, Upper Saddle River, 2002.

Tucker, A., *Applied Combinatorics*, 2d ed., Wiley, New York, 1984.

Uspensky, J. V., and Heaslet, M. A., *Elementary Number Theory*, McGraw-Hill, New York, 1939.

van der Waerden, B. L., *Geometry and Algebra in Ancient Civilizations*, Springer-Verlag, New York, 1983.

———, *A History of Algebra*, Springer-Verlag, New York, 1985.

———, *Modern Algebra*, 4th ed., Ungar, New York, 1966.

———, *Science Awakening*, Wiley, New York, 1963.

Weyl, H., *Symmetry*, Princeton University Press, 1952.

Zariski, O., and Samuel, P., *Commutative Algebra*, volume II, von Nostrand, Princeton, 1960.

索　　引

索引中的页码为英文原书页码，与书中页边标注的页码一致.

A

Abel, N. H.（阿贝尔），125，449，468
abelian group（阿贝尔群），126
  finite（有限阿贝尔群），486
  finitely generated（有限生成的阿贝尔群），190
  free（自由阿贝尔群），487
  primary（准素的阿贝尔群），479
ACC（升链条件），535
action（作用）
  group（群作用），195
    transitive（可迁的群作用），197
  pseudocode，A-4
addition theorem（加法定理），25
adjoining，299，451
adjoint（伴随）
  linear transformation（伴随线性变换），369
  matrix（伴随矩阵），386
Adleman, L.（艾德曼），72
affine group（仿射群），132
al-khwarizmi，34
algebra over a field（域上的代数），540
algebraic，341，451
algebraic integer（代数整数），282
algebraic set（代数集），542
  irreducible（不可约的代数集），552
  projective（射影代数集），556
algebraically closed，301
Alhazen，7，15
alphabet，400
alternating group（交错群），150
anagram（字谜游戏），23
antanairesis（希腊语，辗转相除法），47
anthyphairesis（希腊语，辗转相除法），47
arithmetic mean（算术平均数），10
arrangement，106
Artin, E（阿廷），454
ascending chain condition（升链条件），535
assignment，A-3
associates，227，525
associative，126
  generalized，133
automorphism（自同构）
  field（域的自同构），453
  group（群的自同构），171
axis of reflection（反射的轴），140

B

b-adic digits（*b* 进制数），50
Bachet de Méziriac（梅齐利亚克），51
back diagonal（反对角线），310
ball（球），430
Barr, M.（巴尔），15
base *b*（底 *b*），50
base step（基础步骤），5
basis（基）
  free abelian group（自由阿贝尔群的基），488
  ideal（理想的基），535
  orthonormal（正交基），383
  standard（标准基），329
  vector space（向量空间的基），331
basis theorem（基定理）
  finite abelian groups（有限阿贝尔群的基定理），484
  Hilbert（希尔伯特基定理），539
BCH code（BCH 码），419
Beltrami, E.（贝尔特拉米），552
bijection（双射），94
binary code（二进制码），400
binomial coefficients（二项式系数），20
  q-（二项式系数），500
binomial theorem（二项式定理）
  commutative rings（交换环上的二项式定理），222
  in Z（整数环上的二项式定理）22
block code（分组码），400

Boole，G.（布尔），130
Boolean group(布尔群)，130
Boolean ring(布尔环)，229
Bose，R. C.（博泽），309，417
bracelet(镯)，216
Bruck，R. H.（布拉克），319
Bruck-Ryser theorem(布拉克-黎生定理)，319
Buchberger's algorithm(布切贝哥算法)，576
Buchberger's theorem(布切贝哥定理)，574
Buchberger，B.（布切贝哥），558，570
built from，356
Burnside's lemma(伯恩赛德引理)，209
Burnside，W.（伯恩赛德），209，489

C

calendar formula(日历公式)，80
  Conway，J. H.(康威日历公式)，82
cancellation law(消去律)
  domain(整环上的消去律)，223
  group(群上的消去律)，128
  symmetric group(对称群上的消去律)，107
Cantor，G.（康托尔），97
Cardano formula(卡尔达诺公式)，438
Cardano，G.（卡尔达诺），434
cartesian product(笛卡儿积)，88
casting out 9s(弃九法)，65
casus irreducibilis(不可约情形)，461
Cauchy theorem(柯西定理)，200，202
Cauchy，A.（柯西），107
Cayley theorem(凯莱定理)，192
Cayley，A.（凯莱），149，192，194
Cayley-Hamilton theorem(凯莱-哈密顿定理)，396
center(中心)
  group(群的中心)，166
  matrix ring(矩阵环的中心)，380
centerless(无中心的)，166
centralizer(中心化子)，198
century year(世纪年)，76
characteristic(特征)，295
characteristic polynomial(特征多项式)，389
Chaudhuri
  see Ray-Chaudhuri，417
Chen，J. R.（陈景润），3
chessboard(棋盘)，215
Chinese Remainder Theorem(孙子定理(中国剩余定理))
  commutative rings(交换环上的中国剩余定理)，524
  in Z (整数环上的中国剩余定理)，68
  polynomials(多项式环上的中国剩余定理)，304
circle operation(圈运算)，234
circle group(圆群)，129
class equation(类方程)，201
closed sets(闭集)，545
closed under operation(在运算下封闭)，147
code(码)
  (n, M, d)-code[(n, M, d)-码]，404
  $[n, m]$ code($[n, m]$码)，400
  BCH(BCH 码)，419
  binary(二进制码)，400
  block(分组码)，400
  cyclic(循环码)，414
  dual(对偶码)，412
  Hamming $[2^\ell-1, 2^\ell-1-\ell]$(汉明$[2^\ell-1, 2^\ell-1-\ell]$-码)，411
  Hamming[7，4](汉明 [7，4]-码)，411
  linear(线性码)，406
  parity check(奇偶性检验码)，400
  perfect(完备码)，431
  permutation equivalent，408
  public key cryptography，72
  Reed-Solomon(理德-索罗门码)，421
  triple repetition(三重重复码)，400
  two-dimensional parity(二维奇偶性码)，401
codeword(码字)，400
coefficients(系数)，236
cofactor(余子式)，386
colon ideal(冒号理想)，524
coloring，211
column space(列空间)，327
combinatorial proof，24
common divisor(公因数(公因子，公因元))
  in Z，(整数环Z 上的公因数)，39
    several integers(多个整数的公因数)，54
  in $k[x]$(多项式环 $k[x]$中的公因式)，257
common multiple(公倍数(式))

in Z(整数环中的公倍数)，57
two polynomials(两个多项式的公倍式)，261
common year(普通年(份))，76
commutative(交换的)，126
commutative ring(交换环)，219
domain(整环)，223
Euclidean ring(欧氏环)，267
field(域)，230
local，524
noetherian(诺特环)，536
polynomials(多项式环)，241
principal ideal domain(主理想整环)，260
UFD(唯一分解整环)，526
commutator subgroup(换位子群)，192
companion matrix(相伴矩阵)，398
compass(圆规)，355
complement(补)
abelian group(阿贝尔群中的补)，476
orthogonal(正交补)，326
subset(补子集)，86
subspace(补子空间)，343
complete factorization(完全分解)，113
complete orthogonal set(完全正交集)，316
complex numbers(复数)
conjugate(共轭的复数)，24
exponential form(复数的指数形式)，29
modulus(复数的模)，24
polar decomposition(复数的极分解)，24
root of unity(复数的单位根)，29
composite(合成)
function(函数的合成)，92
number(合数)，2
congruence mod m(模 m 同余)，59
congruence class(同余类)，100，291
conjugacy class(共轭类)，198
conjugate(共轭的)
complex(共轭的复数)，24
group elements(共轭的群元素)，165
subgroups(共轭子群)，491
conjugation，165
consistent system(相容的方程组)，353
constant(常数)
term(常数项)，240
function(常值函数)，88
polynomial(常数多项式)，240
constructible(可构作的)
number(可构作的数)，356
point(可构作的点)，356
subfield of all(可构作的数构成的子域)，357
content(多项式的)(容度)，284，530
continuous(连续的)，557
contrapositive(逆否命题)，4
converse(逆元，逆命题)，28
Conway，J. H.(康威)，82
coordinate list(坐标表)，332
coordinate ring(坐标环)，545
coprime ideals(互素的理想)，524
correct errors(纠错)，404
correspondence theorem(对应定理)
groups(群的对应定理)，184
rings(环的对应定理)，519
coset(陪集)
in group(群中的陪集)
left(群中的左陪集)，154
right(群中的右陪集)，154
in ring(环中的陪集)，292
coset leader(陪集的头字)，423
countable(可数的)，97
cubic(三次的)，240
cubic formula(三次公式)，438
cycle，108
cycle index(圈指数)，213
cycle structure(圈结构)，116
cyclic code(循环码)，414
generating matrix(循环码的生成矩阵)，416
generating polynomial(循环码的生成多项式)，415
cyclic group(循环群)，150，257
cyclotomic polynomial(分圆多项式)，31

D

day，76
De Moivre theorem(棣莫弗定理)，26
De Moivre，A.，26
de Morgan laws(模律)，104

de Morgan A.(摩根), 104
Dean, R. A., 234
decoding, 406
Dedekind, R. 277
degenerate, 325
degree(次数)
  extension field(扩域的次数), 340, 450
  polynomial(多项式的次数)
    one variable(一元多项式的次数), 236
    several variables(多元多项式的次数), 561
degree function(次数函数), 267
degree-lexicographic order(次数-字典序), 564
derivative(导数), 242
Descartes, R. (笛卡儿), 88, 433, 442
detect errors(查错), 404
determinant(行列式)
  function(行列式函数), 384
  linear transformation(线性变换的行列式), 388
  matrix(矩阵的行列式), 384
diabolic square(魔方), 312
diagonal(对角线)
  back(反对角线), 310
  matrix(对角矩阵), 392
diagonalizable(可对角化的), 392
difference(of sets)(集合的)(差), 86
differentiable(可微的), 225
dihedral group(二面体群), 144
  infinite(无限二面体群), 513
dimension(维数), 334
direct image(直接像), 98
direct product(直积)
  commutative rings(交换环的直积), 252
  groups(群的直积), 186
direct sum(直和)
  abelian groups(阿贝尔群的直和), 477
    external(阿贝尔群的外直和), 475
    internal(阿贝尔群的内直和), 475
  matrices(矩阵的直和), 398
  vector spaces(向量空间的直和), 343
direct summand(直和项)
  abelian group(阿贝尔群的直和项), 476
  vector space(向量空间的直和项), 343
direction(方位), 504
Dirichlet, P. G. L. (狄利克雷), 63
discriminant(判别式), 440
disjoint permutations(不相交的置换), 111
disjoint subsets(不相交的子集), 86
distance-preserving, 138
distributive law(分配律), 217
divides
  commutative ring, 226
  in **Z**, 39
division algorithm(除法算式)
  in **Z**(**Z** 上的除法算式), 37
  in $k[x]$($k[x]$上的除法算式), 253
  in $k[x_1, \cdots, x_n]$($k[x_1, \cdots, x_n]$上的除法算式), 567
divisor(因子(式))
  commutative ring(交换环中的因子), 226
  in **Z**(**Z** 中的因子式), 39
domain(整环)
  commutative ring, 223
  function(函数的定义域), 88
  PID(主理想整环), 260
  UFD(唯一分解整环), 526
doomsday(审判日), 82
double induction(二次归纳法), 17
dual basis(对偶基), 382
dual code(对偶码), 412
dual space(对偶空间), 382
Dürer, Albrecht, 310

E

echelon(梯形)
  form(阶梯形), 344
    row reduced(行简化阶梯形), 344
  generating matrix(阶梯形生成矩阵), 409
eigenvalue(特征值), 388
eigenvector(特征向量), 388
Eisenstein criterion(爱森斯坦因判别法), 288, 535
Eisenstein, F. G. M. (爱森斯坦因), 288
elementary divisors(初等因子), 486
elementary matrix(初等矩阵), 346
elementary row operations(初等行变换), 345

elimination ideal(消去理想), 578
empty list(空表), 326
empty set(空集), 85
encoding
  block code, 400
  function(编码函数), 406
  linear code, 406
entries of matrix(矩阵的元素), 131
equal(相等)
  functions(函数的相等), 89
  polynomials(多项式的相等), 240
  sets(集合的相等), 85
equivalence class(等价类), 100
equivalence relation(等价关系), 99
error locator
  polynomial(错误定位多项式), 426
  vector(错误定位向量), 425
error vector, 423
etymology(词源)
  abelian(阿贝尔的), 126, 468
  affine(仿射), 132
  algebra(代数), 34
  algorithm(算法), 34
  alternating group(交错群), 150
  arithmetic(算术), 44
  automorphism(自同构), 453
  binomial(二项(式的)), 20
  coefficient(系数), 236
  corollary(推论), xii
  cosine(余弦), 32
  cubic(三次的), 240
  cycle(圈), 109
  degree(次数), 236
  dihedral group(二面体群), 144
  domain(整环), 230
  echelon form(阶梯形), 344
  eigenvalue(特征值), 388
  factor(因子), 14
  factorial(阶乘), 14
  field(域), 230
  Gaussian integers(高斯整环), 268
  golden ratio(黄金分割率), 13
  googol (10^{100}), 75
  Graeco-Latin squares(哥雷可-拉丁方), 315
  homomorphism(同态), 159
  ideal(理想), 277
  induction(归纳), 5
  isomorphism(同构), 159
  kernel(核), 163
  Latin square(拉丁方), 315
  lemma(引理), xii
  mathematics(数学), xii
  matrix(矩阵), 130
  modulo(模), 59
  Nullstellensatz(零点定理), 549
  orthogonal(正交), 325
  polar coordinates(极坐标), 25
  polar decomposition(极分解), 25
  polyhedron(多面体), 144
  polynomial(多项式), 20
  power(方幂), 134
  pure subgroup(纯子群), 480
  quadratic(二次的, 平方的), 240
  quaternions(四元数), 167
  quotient group(商群), 179
  quotient ring(商环), 294
  radical(根的, 根式), 34
  regular representation(正则表示), 207
  ring(环), 219
  root(根), 33
  secant(割线), 32
  September(九月), 78
  signum(正负号数), 121
  sine(正弦), 32
  stochastic(随机的), 147
  tangent(正切), 32
  theorem(定理), xii
  torsion subgroup(挠群), 489
  translation(平移), 140
  variety(簇), 542
  vector(向量), 321
Euclid(欧几里得), 38
Euclid lemma(欧几里得引理)
  in Z (Z中的欧几里得引理), 41

in $k[x]$($k[x]$中的欧几里得引理)，264
Euclidean algorithm(欧几里得算法，欧氏算法)
in Z (Z中的欧氏算法)，45
number of steps(欧氏算法的步数)，46
polynomials，265
Euclidean ring(欧几里得环，欧氏环)，267
Eudoxus(欧多克索斯)，44 354
Euler ϕ-function(欧拉ϕ-函数)，32，43
Euler theorem(欧拉定理)
complex exponentials(复指数的欧拉定理)，29
congruences(同余的欧拉定理)，177
Latin squares(拉丁方的欧拉定理)，309
Euler，L. (欧拉)，305
evaluation homomorphism(赋值同态)，246
evaluation map(赋值影射)，523
even permutation(偶置换)，122
expression(表示)，133
extension field(扩域)，340
algebraic(代数扩域)，341
degree(扩域的次数)，340
finite(有限扩域)，340
Galois(伽罗瓦扩域)，472
normal(正规扩域)，459
pure(单纯扩域)，460
radical(根式扩域)，460
splitting field(分裂域)，451

F

factor groups(商群)，465
factorial(阶乘)，14
Fermat(费马)
theorem(费马定理)，64，176，202
Two-Squares Theorem(费马二平方定理)，272
Fermat primes(费马质数)，365
Fermat's last theorem(费马最后(大)定理)，277
Fermat，P.，64
Ferrari，Lodovici(费拉理)，440
Feynman，R. P. (费伊曼)，440
Fibonacci(斐波那契)，432
Fibonacci sequence(斐波那契序列)，13，398
field(域)，230
15-puzzle(15-游戏)，119
finite dimensional(有限维的)，330
finite extension(有限扩张)，340
finitely generated
abelian group(有限生成的阿贝尔群)，190
ideal(有限生成的理想)，535
Fior，Antonio Maria(费欧)，434
first isomorphism theorem(第一同构定理)
commutative rings(交换环的第一同构定理)，294
groups(群的第一同构定理)，180
vector spaces(向量空间的第一同构定理)，382
fixed variables(固定变量)，351
fixes，108，453
floor(下取整)，28
Fontana，Niccolò(符塔那)，434
FOR，A-5
formal power series over R(R上的形式幂级数)，236
four-group(四元群)，148
fraction field(分式域)，233
Frattini，G. (弗拉蒂尼)，489，499
free abelian group(自由阿贝尔群)，487
free variables(自由变量)，351
frieze group(楣群)，510，512
point group(点群)，512
Frobenius，G. (弗罗贝尼乌斯)，209，490
function(函数)，88
function field(函数域)，241
Fundamental Theorem(基本定理)
Algebra(代数基本定理)，473
Arithmetic(算术基本定理)，55
Finite Abelian Groups(有限阿贝尔群的基本定理)，486
Galois Theory(伽罗瓦理论的基本定理)，472

G

Galois extension(伽罗瓦扩张)，472
Galois group(伽罗瓦群)，454
Galois theorem(伽罗瓦定理)，301
Galois，E. (伽罗瓦)，125，449
Gauss theorem(高斯定理)
R UFD implies $R[x]$ UFD(R是UFD推出$R[x]$是UFD)，531
cyclotomic polynomial (分圆多项式的高斯定

理），288
irreducible polynomials（不可约多项式的高斯定理），285
regular n-gon（正 n-边形的高斯定理），474
Gauss's lemma（高斯引理），283，530
Gauss，C. F.（高斯），7，283
Gauss-wantzel theorem（高斯-万提斯定理），365，474
Gaussian equivalent（高斯等价），348
Gaussian integers（高斯整数环），219
gcd（最大公因子）
commutative ring（交换环中的最大公因子），528
in Z（Z 中的最大公因子），39
several integers（多个整数的最大公因子），54
UFD（UFD 中的最大公因式），529
general linear group（一般线性群），131
generalized associativity（广义结合律），133
generating matrix（生成矩阵），409
echelon（阶梯形生成矩阵），409
generating polynomial（生成多项式），415
generator，cyclic group（生成元），（循环群的生成元），150
generators subgroup（生成子群），153
geometric mean（几何平均数），10
Gherardo of Cremona，33
glide reflection（滑动反射），506
Golay，M. J. E.（哥雷），399
Goldbach's conjecture（哥德巴赫猜想），3
golden ratio（黄金比率），13
Goldman，O.（哥德曼），551
googol（10^{100}），75
Gordan，P.（戈丹），538
greatest common divisor（最大公因子）
domain（整环中的最大公因子），259
in Z （Z 中的最大公因子），39
several integers（多个整数的最大公因子），54
in $k[x]$（$k[x]$中的最大公因式），257
Gregorian calendar（葛里高利历法），76
Gröbner basis（格罗布纳基），570
group（群），126
abelian（阿贝尔群），126
affine（仿射群），132
alternating（交错群），150
Boolean（布尔群），130
circle group（圆群），129
cyclic（循环群），150
dihedral（二面体群），144
infinite（无限二面体群），513
four-group（四元群），148
free abelian（自由阿贝尔群），487
frieze group（楣群），510
Galois（伽罗瓦群），454
general linear（一般线性群），131
integers mod m（整数模 m 的剩余类群），172
orthogonal（正交群），139
p-group（p-群），201，203
parity（奇偶性群），130
quaternions（四元数群），167
quotient（商群），179
simple（单群），203
solvable（可解群），465
special linear（特殊线性群），158
special orthogonal（特殊正交群），131
stochastic（随机群），147
symmetric（对称群），107
symmetry（群的对称性），143
unitriangular（单位上三角群），496
group of units（单位群），228

H

Hadamard product（阿达马积），306
Hadamard，J.（阿达马），306
half-turn（半翻转），508
Hamilton，W. R.（哈密顿），167
Hamming（汉明）
$[2^\ell-1，2^\ell-1-\ell]$code（汉明$[2^\ell-1，2^\ell-1-\ell]$码），411
[7，4] code（汉明[7，4]码），411
bound（汉明界），431
codes，411
distance（汉明距离），403
weight（汉明权），407
Hamming，R. W.（汉明），399，403
Helikon（赫林坎），354

Hermite, C. (埃尔米特), 394
hermitian(埃尔米特)
  form(埃尔米特型), 394
  matrix(埃尔米特矩阵), 398
Heron's formula(海伦公式), H-2
Hilbert, D. (希尔伯特), 219, 538
  basis theorem(希尔伯特基定理), 539
  Nullstellensatz(希尔伯特零点定理), 549
Hocquenghem, A. (霍可汉姆), 417
homogeneous coordinates(齐次坐标)
  projective line(射影直线的齐次坐标), 339
  projective point(射影平面的齐次坐标), 339
homogeneous linear system(齐次线性方程组), 323
homomorphism(同态)
  commutative rings(交换环的同态), 243
  groups(群的同态), 159
    conjugation(群的共轭), 165
    natural map(群的自然映射), 180
Hume, J. (休谟), 433
Hungerbühler, N. (韩格百勒), 362
hyperbolic cosine(双曲线余弦函数), 9

I

ideal(理想), 249
  colon(冒号理想), 524
  elimination(消去理想), 578
  finitely generated(有限生成的理想), 535
  generated by a_1, …, a_n(由 a_1, …, a_n 生成的理想), 535
  maximal(最大理想), 521
  prime(质理想), 519
  principal(主理想), 249
  radical(根理想), 547
identity(单位元)
  function(恒等函数), 88
  group element(群的单位元), 126
  matrix(恒等矩阵), 131
if and only if(当且仅当), 28
IF-THEN-ELSE, A-5
image(像)
  commutative ring(交换环中的像), 248
  function(函数的像), 88
  group(群中像), 88
  linear transformation(线性变换的像), 376
inclusion(包含), 89
independent list(无关的表), 331
  longest(最长的无关表), 335
indeterminate(未定元), 239
index(指数)
  cycle(圈的指数), 213
  subgroup(子群的指数), 156
indirect proof(间接的证明), 4
induction(归纳法), 5
  base step(归纳法的基础步骤), 5
  double(双归纳法), 17
  inductive hypothesis(归纳假设), 6
  inductive step(归纳步骤), 5
  second form(第二归纳法), 11
inductive reasoning(归纳的解释), 1
inequality of the means(平均数的不等式), 11
infinite dimensional(无限维数), 330
infinite order(无限阶), 136
injective(单射), 91
inner product(内积), 325
  nondegenerate(非退化的内积), 325
integer(整数), 1
integers mod m(整数模 m), 172
integral domain(整环), 223
interpolation, Lagrange(拉格朗日插值, 257
intersection(交), 85
invariance of dimension(维数不变性), 334
invariant of group(群的不变性), 162
inverse(逆)
  2×2 matrix(2×2 矩阵的逆矩阵), 131
  function(反函数), 95
  group element(群元素的逆元素), 128
  image(逆像), 98
  in commutative ring(交换环中的逆元素), 227
  matrix(逆矩阵), 325
invertible matrix(可逆矩阵), 386
irreducible(不可约的)
  algebraic set(不可约的代数集), 552
  in $k[x]$($k[x]$中的不可约元), 262
  in commutative ring(交换环中的不可约元), 526

polynomial(不可约的多项式), 262
irredundant intersection(无赘交), 554
irredundant union(无赘并), 553
isometry(等距同构), 138
glide reflection(滑动反射), 506
half-turn(半反转), 508
reflection(反射), 501
rotation(旋转), 501
translation(平移), 501
isomorphism(同构)
commutative rings(交换环的同构), 243
groups(群的同构), 159
vector spaces(向量空间的同构), 366

J

Jordan, C. (约当), 490
Julian calendar(儒略历法), 76

K

kernel(核)
group homomorphism(群同态的核), 163
linear transformation(线性变换的核), 376
ring homomorphism(环同态的核), 248
Khayyam, Omar(奥姆), 432
Klein group(克莱因群), 148
Klein, F. (克莱因), 144
Kronecker(克罗内克)
delta(克罗内克 δ 函数), 369
product(克罗内克积), 308
theorem(克罗内克定理), 300
Kronecker, L. (克罗内克), 44, 490
Krull, W. (克鲁尔), 551
Kummer, E. (库默尔), 277

L

Lagrange interpolation(拉格朗日插值), 257
Lagrange theorem(拉格朗日定理), 156
Lagrange, J. -L. (拉格朗日), 156
Lam, C. (勒姆), 319
Lamé theorem(拉梅定理), 49
Lamé, G. (拉梅), 49
Laplace expansion(拉普拉斯展开), 385
Laplace, P. -S. (拉普拉斯), 385
Latin square(拉丁方), 305
diagonal(对角的拉丁方), 313
law of substitution(替换律), 125
laws of exponents(指数律), 135
lcm, (最小公倍数)
in Z (整数的最小公倍数), 57
polynomials(多项式的最小公倍数), 261
leading(首项)
coefficient(首项系数), 236
column(首列), 344
entry(首元), 344
term(首项), 253
leap year(润年), 76
least common multiple
in Z, 57
polynomials, 261
least criminal(最小反例), 3
least integer axiom(最小整数公理), 3
Leibniz, G. W. (莱布尼茨), 36
length of cycle(循环的长度), 108
Leonardo da Vinci(莱昂纳多·达·芬奇), 509
Leonardo of Pisa
see Fibonacci, 432
Levi ben Gershon, 4
lexicographic order(字典顺序), 561
Lindemann, F. (林德曼), 341
linear code(线性码), 406
linear combination(线性组合), 327
commutative ring(交换环中的线性组合), 227
in Z (Z 中的线性组合), 40
vector space(向量空间中的线性组合), 327
linear polynomial(线性多项式), 240
linear system(线性方程组), 323
homogeneous(齐次线性方程组), 323
linear transformation(线性变换), 366
adjoint(相伴的线性变换), 369
nonsingular(非退化的线性变换), 366
orthogonal(正交的线性变换), 383
linearly dependent(线性相关), 331
linearly independent(线性无关), 331

list(表)，106，326
local ring(局部环)，524
longest independent list(极大无关组)，335
loop(圈)
FOR，A-5
REPEAT，A-4
WHILE，A-3
lowest terms(既约形式)
in Q (Q 中元的既约形式)，43
in $k(x)$($k(x)$中元的既约形式)，264

M

magic number(幻数)，310
magic square(幻方)，310
diabolic square(魔方)，312
Mann，A. (曼)，202
Mars(火星)，399
Mascheroni，L. (马斯凯罗尼)，362
matrix(矩阵)，130
adjoint(伴随矩阵)，386
echelon form(矩阵的阶梯形矩阵)，345
elementary(初等矩阵)，346
generating(生成矩阵)，409
hermitian(厄尔米特矩阵)，398
inverse(逆矩阵)，325
invertible(可逆矩阵)，386
linear transformation(线性变换的矩阵)，369
nilpotent(幂零矩阵)，399
nonsingular(非退化的矩阵)，325
orthogonal(正交矩阵)，383
permutation(置换矩阵)，170
row reduced echelon form(行简化的阶梯形矩阵)，344
scalar(数量矩阵)，380
symmetric(对称矩阵)，324
transpose(矩阵的转置)，324
triangular(三角矩阵)，353
Vandermonde(范德蒙德矩阵)，397
Maurolico，F. (茂儒里克)，4
maximal element(极大元素)，
in family of ideals(理想集中的极大元)，536
in partially ordered set(偏序集中的极大元)，537
maximal ideal(最大理想)，521
maximum condition(最大条件)，536
Mayan calendar(玛雅历法)，70
McIver，A.，195
McKay，J. H.，202
metric(度量)，402
minimum distance(最小距离)，404
modulus(模)
complex number(复数的模)，24
congruence(同余中的模)，59
Mohr，G. (蒙荷)，362
monic polynomial(首一多项式)，240
several variables(多变量的首一多项式)，561
monomial ideal(单项式理想)，569
monomial order(单项式序)，560
degree-lexicographic order(次数-字典序)，564
lexicographic order(字典序)，561
Moore theorem(穆尔定理)，457
Moore，E. H. (穆尔)，457
Motzkin，T. S.，270
moves，108
multidegree(多重次数)，559
multiple(倍数(式))
commutative ring(交换环中的倍式)，226
in Z (Z 中的倍数)，39
multiplication table(乘法表)，160
multiplicity(重数)，227

N

natural map(自然映射)
groups(群的自然映射)，180
rings(环的自然映射)，293
vector spaces(向量空间的自然映射)，382
natural numbers(自然数)，1
n choose r(n 中选 r)，20
nearest codeword(最近的字)，404
needs no parentheses(无需括号)，133
Neumann，B. H. (诺伊曼)，158
Neumann，P. M. (诺伊曼)，195
Newton's method(牛顿法)A-4
nilpotent(幂零)，242
element(幂零元素)，547
matrix(幂零矩阵)，399

nilradical(幂零根), 556
Noether, E. (诺特), 180, 454, 536
noetherian(诺特环), 536
nondegenerate(非退化的), 325
nonempty(非空的), 3
nongenerator(非生成元), 489
nonsingular(非奇异的)
  linear transformation(非奇异的线性变换), 366
  matrix(非奇异的矩阵), 131, 325
nontrivial subgroup(非平凡的子群), 148
norm(范数), 268
normal(正规的)
  extension(正规扩张), 459
  series(正规序列), 465
  subgroup(正规子群), 164
normalizer(正规化子), 491
Nullstellensatz(零点定理), 549
  weak(弱零点定理), 548

O

O'Brien, E. (欧布莱恩), 194
odd permutation(奇置换), 122
one(in commutative ring)((交换环中的)单位元), 219
one-one correspondence
  see bijection(一一映射), 94
one-to-one
  see injective(单射), 91
onto(function)
  see surjective(满射), 90
operation(作用), 125
orbit(轨道), 197
order(阶)
  group(群的阶), 151
  group element(群元素的阶), 136
    infinite(无限阶的元), 136
Oresme, N. , 16
origin(原点), 356
orthogonal(正交的)
  complement(正交补)326
  group(正交群), 139
  group $O(2, \mathbb{R})$(正交群 $O(2, \mathbb{R})$), 142
  Latin squares(正交的拉丁方), 307
    set(正交集), 315
  matrix(正交矩阵), 383
  transformation(正交变换), 383
orthonormal basis(正交规范基), 383
Oughtred, W. (奥奇德), 433

P

p-adic metric(p-度量), 58, 403
p-adic norm(p-范数), 58
p-group(p-群), 201, 203
p-primary abelian group(p-准素的阿贝尔群), 479
pairwise disjoint(两两不交), 102
pairwise relatively prime(两两互素), 278
Pappus(帕普斯), 344
parallelogram law(平行四边形定律), 321
parity(奇偶性)
  binary word(二元码的奇偶性), 400
  permutation(置换的奇偶性), 122
  same(同奇偶性), 59
parity check code(奇偶性检验码), 400
parity check matrix(奇偶性检验矩阵), 412
parity group(奇偶性群), 130
Parker, E. T. (帕克), 309
partial fractions(部分分式), 279
partially ordered set(偏序集), 537
partition(划分), 102
partition notation, 407
partition of n(n 的划分), 488
Pascal theorem(帕斯卡定理), 21
Pascal's triangle(帕斯卡三角形), 18
Pascal, B. (帕斯卡), 18
Pell's equation(佩尔定理), 2
perfect code(完备码), 431
perfect squares(完全平方), 2
permutation(置换), 106
  complete factorization(置换的完全分解), 113
  cycle(循环置换), 108
  disjoint(不交的置换), 111
  even(偶置换), 122
  odd(奇置换), 122
  order(置换的阶), 137
  parity(置换的奇偶性), 122

regular(正则置换)，124
signum(置换的符号)，121
transposition(对换)，108
permutation equivalent codes(置换等价的码)，408
permutation matrix(置换矩阵)，170
PID(主理想整环)，260
pigeonhole principle(鸽巢原理)，105
Plato(柏拉图)，354
Pogrebishte，83
point group(点群)，512
polar coordinates(极坐标)，25
polar decomposition(极分解)，24
Pólya，G.（波利亚)，214
Pólya theorem(波利亚定理)，214
polynomial(多项式)
n variables(n 元多项式)，241
cyclotomic(分圆多项式)，31
equality(多项式的相等)，240
function(多项式函数)，240，541
irreducible(不可约多项式)，262
leading term(多项式的首项)，253
monic(首一多项式)，240
solvable by radicals(根式可解的多项式)，460
zero(零多项式)，236
polynomial over R(R 上的多项式)，236
powers(方幂)，134
predecessor(先导)，11
primary component(准素分支)，479
prime(素数)
field(素域)，234
ideal(素理想)，519
number(素数)，2
primitive element(本原元)，301
primitive polynomial(本原多项式)，283，529
primitive root of unity(本原单位根)，31
principal ideal(主理想)，249
principal ideal domain(主理想整环)，260
projective algebraic set(射影代数集)，556
projective plane(射影平面)，317，337，338
order n(n 元的射影平面)，318，337
proof by contradiction，4
proper
divisor(真因子)，525
ideal(真理想)，249
subgroup(真子群)，148
subset(真子集)，85
subspace(真子空间)，323
pseudocode(伪码)，A-3
action(作用)，A-4
assignment，A-3
branching structure(枝结构)
IF-THEN-ELSE，A-5
loop(圈)
FOR，A-5
REPEAT，A-4
WHILE，A-3
public key cryptography(公开密钥密码学)，72
pure extension(单纯扩张)，460
pure subgroup(纯子群)，480
Pythagorean triple(毕达哥拉斯数)，55
primitive(本原的毕达哥拉斯数)，55

Q

q-binomial coefficients(q-二项式系数)，500
quadratic(二次的)，240
quartic(四次的)，240
quartic formula(四次公式)，442
quaternions(四元数)，167
quintic(五次的)，240
quotient(商，商式)
division algorithm(除法算式中的商式)
Z(Z 中的商)，38
polynomials(多项式的商)，254
group(商群)，179
ring(商环)，292
space(商空间)，343

R

radical(根，根式)
extension(根式扩张)，460
ideal(根理想)，547
of ideal(理想的根)，547
tower(根式塔)，460

Rahn, J. H(拉恩), 433
Ramon the raccoon, 66
rank of matrix(矩阵的秩), 346
rate of information(信息率), 406
rational functions(有理函数), 233, 241
Ray-Chaudhuri, D. K. (雷-丘德贺理), 417
r-cycle(r-循环), 108
Recorde, R. (理科德), 433
reduced basis(简化基), 578
reduced mod $\{g_1, \cdots, g_m\}$(简化的 mod $\{g_1, \cdots, g_m\}$), 567
reduced polynomial(简化的多项式), 435
reduction(简化), 565
Reed, I. S. (理德), 421
Reed-Solomon code(理德-索罗门码)
  t-error correcting(纠 t-错的理德-索罗门码), 421
reflection(反射), 140, 501
regular(正则)
  permutation(正则置换), 124
  representation(正则表示), 207
relation(关系), 99
relatively prime(互素)
  in Z(Z 中的互素), 42
  polynomials(多项式的互素), 264
  UFD(UFD 中的互素), 529
remainder(余, 余式)
  division algorithm(除法算式的余式)
    in Z(Z 的除法算式的余式), 38
    polynomials(多项式的除法算式的余式), 254
  mod G(模 G 的余), 568
REPEAT, A-4
repeated roots(重根), 274
representation on cosets(陪集上的表示定理), 193
restriction(限制), 89
ring(环)
  commutative(交换环), 219
  noncommutative(非交换环), 220
  zero(零环), 223
ring of formal power series(形式幂系列环), 243
ring of polynomials(多项式环), 238
Rivest, R. (瑞斯特), 72
root(根), 255
  multiplicity(根的重数), 277
root of unity(单位根), 29, 452
  primitive(本原单位根), 31
rotation(旋转), 139, 501
roulette wheel(滚轮), 215
row space(行空间), 327
RSA public key cryptography, 72
Ruffini, P. (鲁费尼), 449
ruler(直尺), 355
Ryser, H. J. (黎生), 319

S

same number(基数相同), 97
same parity(奇偶性相同), 122
Sarges, H. (萨杰斯), 538
Saturn(土星), 399
scalar(纯量), 321
  matrix(纯量矩阵), 170, 380
  multiplication(纯量乘法), 320
  transformation(纯量变换), 380
Schering, E. (师林), 490
Scipione del Ferro(费罗), 433
second form of induction(第二归纳法), 11
second isomorphism theorem(第二同构定理), 183
semigroup(半群), 133
separable(可分的)
  extension(可分扩张), 471
  polynomial(可分多项式), 471
Shalev D. (谢勒夫), 134
Shamir. A. (沙米尔), 72
Shannon, C. E. (香农), 399
Shrikhande, S. S. (施理克汉德), 309
Sierpinski, W., 2
signum(符号), 121
similar matrices(相似矩阵), 375
simple group(单群), 203
simple move, 15 game(单动), 119
Singer, R. (辛格), 288
single-valued(单值), 91
Singleton bound(单字界), 430
Singleton, R. C., 430
singular(退化的), 378

skew symmetric(斜对称的)，342
smallest subspace(最小子空间)，328
Solomon，G.（索罗门)，421
solution(解)
  linear system(线性方程组的解)，323
  set(解集)，323
  space(解空间)，324
solution space，327
solvable by radicals(根式可解)，460
solvable group(可解群)，465
spans，327
Spec(R)，557
special linear group(特殊线性群)，158
special orthogonal group(特殊正交群)，131
splits(分裂)，300，451
splitting field(分裂域)，451
S-polynomial(S-多项式)，572
squarefree integer(无平方因子的整数)，54
stabilizer(稳定化子)，197
standard basis(标准基)，329
Steinitz，E.（施特尼兹)，473
Stickelberger，L.（施蒂克贝格)，490
stochastic group(随机群)，147
straightedge(直边)，355
subfield(子域)，233
subgroup(群)，148
  center(群的中心)，166
  commutator(换位子群)，192
  cyclic(循环子群)，150
  generated by subset(由集合生成的子群)，153
  nontrivial(非平凡的子群)，148
  normal(正规子群)，164
  proper(真子群)，148
  pure(纯子群)，480
  Sylow(西罗子群)，490
subring(子环)，223
subset(子集)，85
subspace(子空间)，322
  proper(真子空间)，323
  row space(行子空间)，327
  smallest(最小的子空间)，328
  spanned by X(由 X 生成的子空间)，327
subtraction(减法)，222
summand，direct(直和的项)，476
support(支撑)，407
surjective(满射)，90
Sylow subgroup(西罗子群)，490
Sylow theorem(西罗定理)，492，493
Sylow，L.（西罗)，490
symmetric difference(对称差)，104
symmetric group(对称群)，107
symmetric matrix(对称矩阵)，324
symmetry(对称)，143
symmetry group(对称群)，143
syndrome(和声)，423
syndrome matrix(和声矩阵)，427

T

target(目标域)，88
Tarry，G.（泰利)，309
Tartaglia(塔尔塔利亚)，434
third isomorphism theorem(第三同构定理)，183
topological space(拓扑空间)，545
topology(拓扑)，545
torsion subgroup(挠子群)，489
total degree(全次数)，559
trace(迹)，391
transcendental(超越元)，341
transition matrix(过渡矩阵)，369
transitive(传递性)
  equivalence relation(等价关系中的传递性)，99
  group action(群作用的传递性)，197
translation(平移)，140
transpose，324
transposition(对换)，108
triangle inequality(三角不等式)，402
triangular matrix(三角矩阵)，353
tridiagonal matrix(三对角矩阵)，397
triple repetition code(三重重复码)，400
two-squares theorem(二平方定理)，272
type，pure extension(单纯扩张中的型)，460

U

UFD(唯一分解整环)，526

uncountable(不可数)，97
union(并)，86
unique(唯一)，12
unique factorization(唯一分解)，275
unique factorization domain(唯一分解整环)，526
unit(单位)，227
unitriangular(单位上三角)，496

V

van der Waerden，B. L.(范德瓦尔登)，44，354
Vandermonde matrix(范德蒙德矩阵)，397
Vandermonde，A. -T.，397
variables(变量)
  fixed(固定变量)，351
  free(自由变量)，351
variety(簇)，552
vector space(向量空间)，320
vectors(向量)，321
Viète，F. (韦达)，433，446

W

Wantzel，P. L. (万提斯)，362
weighing，52
well-defined(定义良好的)，103
well ordered(良序的)，560
WHILE，A-3
Widman，J. (魏德曼)，433
Wielandt，H.(维兰特)，494
Wiles，A. (威尔斯)，277
Williams，K. S.，270
Wilson's theorem(威尔逊定理)，177
Wilson，J.(威尔逊)，177
word(字)，400

Y

year(年)，76
  century year(世纪年)，76
  leap year(闰年)，76

Z

Zariski topology(扎里斯基拓扑)
  on k^n(k^n 上的扎里斯基拓扑)，545
  Spec(R) (Spec(R)中的扎里斯基拓扑)，557
Zariski，O. (扎里斯基)，557
zero(零)
  polynomial(多项式的零点)，236
  ring(环的零点)，223
  several variables(多变量多项式的零点)，542
zero set of vector(向量的零集)，407
Zorn's lemma(佐恩引理)，538